



**Security Products**

# **SSG 20 Hardware Installation and Configuration Guide**

**Juniper Networks, Inc.**

1194 North Mathilda Avenue  
Sunnyvale, CA 94089

USA

408-745-2000

**[www.juniper.net](http://www.juniper.net)**

Part Number: 530-015646-01, Revision 03

## Copyright Notice

Copyright © 2006 Juniper Networks, Inc. All rights reserved.

Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. All specifications are subject to change without notice. Juniper Networks assumes no responsibility for any inaccuracies in this document or for any obligation to update information in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

## FCC Statement

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. The equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Juniper Networks' installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Consult the dealer or an experienced radio/TV technician for help.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.

**Caution:** Changes or modifications to this product could void the user's warranty and authority to operate this device.

## Disclaimer

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR JUNIPER NETWORKS REPRESENTATIVE FOR A COPY.

# Table of Contents

	<b>About This Guide</b>	<b>5</b>
	Organization .....	6
	WebUI Conventions .....	6
	CLI Conventions .....	7
	Obtaining Documentation and Technical Support .....	8
<b>Chapter 1</b>	<b>Hardware Overview</b>	<b>9</b>
	Port and Power Connectors .....	10
	Front Panel .....	11
	System Status LEDs .....	11
	Port Descriptions .....	13
	Ethernet Ports .....	13
	Console Port .....	13
	AUX Port .....	14
	Mini Physical Interface Module Port Descriptions .....	14
	Back Panel .....	16
	Power Adapter .....	16
	Radio Transceivers .....	16
	Grounding Lug .....	17
	Antennae Types .....	18
	USB Port .....	18
<b>Chapter 2</b>	<b>Installing and Connecting the Device</b>	<b>19</b>
	Before You Begin .....	20
	Installing Equipment .....	20
	Connecting Interface Cables to a Device .....	22
	Connecting the Power .....	22
	Connecting a Device to a Network .....	23
	Connecting a Device to an Untrusted Network .....	23
	Ethernet Ports .....	24
	Serial (AUX/Console) Ports .....	24
	Connecting Mini PIMs to an Untrusted Network .....	24
	ADSL2/2+ Mini PIM .....	24
	ISDN, T1, E1, and V.92 Mini PIMs .....	25
	Connecting a Device to an Internal Network or a Workstation .....	25
	Ethernet Ports .....	25
	Wireless Antennae .....	26
<b>Chapter 3</b>	<b>Configuring the Device</b>	<b>27</b>
	Accessing a Device .....	28
	Using a Console Connection .....	28
	Using the WebUI .....	29

	Using Telnet .....	30
	Default Device Settings .....	31
	Basic Device Configuration .....	33
	Root Admin Name and Password .....	33
	Date and Time .....	34
	Bridge Group Interfaces .....	34
	Administrative Access .....	35
	Management Services .....	35
	Hostname and Domain Name .....	36
	Default Route .....	36
	Management Interface Address .....	36
	Backup Untrust Interface Configuration .....	37
	Basic Wireless Configuration .....	37
	Mini PIM Configuration .....	41
	ADSL2/2 + Interface .....	41
	Virtual Circuits .....	42
	VPI/VCI and Multiplexing Method .....	42
	PPPoE or PPPoA .....	43
	Static IP Address and Netmask .....	44
	ISDN Interface .....	45
	T1 Interface .....	45
	E1 Interface .....	46
	V.92 Modem Interface .....	47
	Basic Firewall Protections .....	48
	Verifying External Connectivity .....	48
	Resetting a Device to Factory Defaults .....	49
<b>Chapter 4</b>	<b>Servicing the Device</b>	<b>51</b>
	Required Tools and Parts .....	51
	Replacing a Mini-Physical Interface Module .....	51
	Removing a Blank Faceplate .....	52
	Removing a Mini PIM .....	52
	Installing a Mini PIM .....	53
	Upgrading Memory .....	54
<b>Appendix A</b>	<b>Specifications</b>	<b>57</b>
	Physical .....	58
	Electrical .....	58
	Environmental Tolerance .....	58
	Certifications .....	59
	Safety .....	59
	EMC Emissions .....	59
	EMC Immunity .....	59
	ETSI .....	59
	T1 Interface .....	60
	Connectors .....	60
<b>Appendix B</b>	<b>Initial Configuration Wizard</b>	<b>63</b>
	<b>Index</b> .....	<b>85</b>

# About This Guide

The Juniper Networks Secure Services Gateway (SSG) 20 device is an integrated router and firewall platform that provides Internet Protocol Security (IPSec) virtual private network (VPN) and firewall services for a branch office or a retail outlet.

Juniper Networks offers two models of the SSG 20 device:

- SSG 20, which supports auxiliary (AUX) connectivity
- SSG 20-WLAN, which supports integrated 802.11a/b/g wireless standards

Both SSG 20 devices support universal serial bus (USB) storage and two mini physical interface module (PIM) slots that can hold any of the mini PIMs. The devices also provide protocol conversions between local area networks (LANs) and wide area networks (WANs).

---

**NOTE:** The configuration instructions and examples in this document are based on the functionality of a device running ScreenOS 5.4. Your device might function differently depending on the ScreenOS version you are running. For the latest device documentation, refer to the Juniper Networks Technical Publications website at <http://www.juniper.net/techpubs/hardware>. To see which ScreenOS versions are currently available for your device, refer to the Juniper Networks Support website at <http://www.juniper.net/customers/support/>.

---

## Organization

---

This guide contains the following sections:

- Chapter 1, “Hardware Overview,” describes the chassis and components of an SSG 20 device.
- Chapter 2, “Installing and Connecting the Device,” describes how to mount an SSG 20 device and how to connect cables and power to the device.
- Chapter 3, “Configuring the Device,” describes how to configure and manage an SSG 20 device and how to perform some basic configuration tasks.
- Chapter 4, “Servicing the Device,” describes service and maintenance procedures for the SSG 20 device.
- Appendix A, “Specifications,” provides general system specifications for the SSG 20 device.
- Appendix B, “Initial Configuration Wizard,” provides detailed information about using the Initial configuration Wizard (ICW) for an SSG 20 device.

## WebUI Conventions

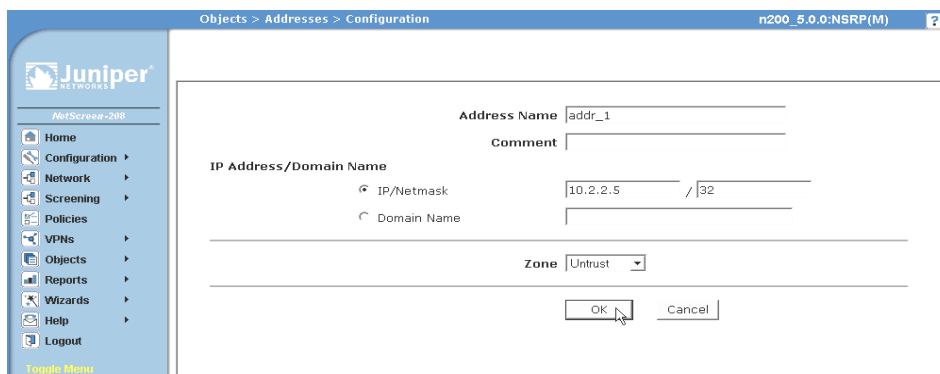
---

To perform a task with the WebUI, you first navigate to the appropriate dialog box, where you then define objects and set parameters. A chevron ( > ) shows the navigational sequence through the WebUI, which you follow by clicking menu options and links. The set of instructions for each task is divided into navigational path and configuration settings.

The following figure lists the path to the address configuration dialog box with the following sample configuration settings:

Objects > Addresses > List > New: Enter the following, then click **OK**:

Address Name: addr\_1  
IP Address/Domain Name:  
    IP/Netmask: (select), 10.2.2.5/32  
Zone: Untrust

**Figure 1: Navigational Path and Configuration Settings**

## CLI Conventions

The following conventions are used to present the syntax of CLI commands in examples and in text.

In examples:

- Anything inside square brackets [ ] is optional.
- Anything inside braces { } is required.
- If there is more than one choice, each choice is separated by a pipe ( | ). For example:

```
set interface { ethernet1 | ethernet2 | ethernet3 } manage
```

means “set the management options for the ethernet1, the ethernet2, or the ethernet3 interface.”

- Variables are in *italic* type:

```
set admin user name1 password xyz
```

In text:

- Commands are in **boldface** type.
- Variables are in *italic* type.

---

**NOTE:** When entering a keyword, you need to type only enough letters to identify the word uniquely. For example, typing **set adm u kath j12fmt54** is enough to enter the command **set admin user kathleen j12fmt54**. Although you can use this shortcut when entering commands, all the commands documented here are presented in their entirety.

---

## Obtaining Documentation and Technical Support

---

To obtain technical documentation for any Juniper Networks product, visit [www.juniper.net/techpubs/](http://www.juniper.net/techpubs/).

For technical support, open a support case using the Case Manager link at <http://www.juniper.net/support/> or call 1-888-314-JTAC (within the United States) or 1-408-745-9500 (outside the United States).

If you find any errors or omissions in this document, please contact us at the following email address:

[techpubs-comments@juniper.net](mailto:techpubs-comments@juniper.net)



## Chapter 1

# Hardware Overview

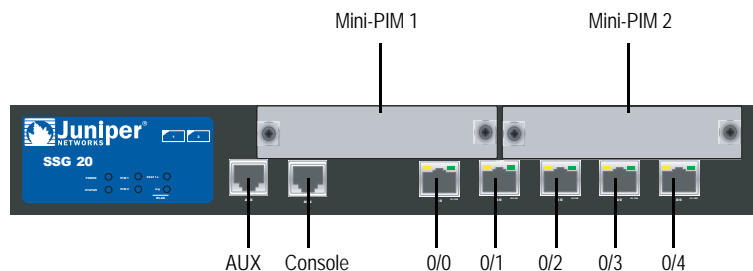
This chapter provides detailed descriptions of the SSG 20 chassis and its components. It contains the following sections:

- “Port and Power Connectors” on page 10
- “Front Panel” on page 11
- “Back Panel” on page 16

## Port and Power Connectors

This section describes and displays the location of the built-in ports and power connectors. Refer to the following figure for built-in port locations and Table 1 for the power connector descriptions.

**Figure 2: Built-in Port and Mini-PIM Location**



**Table 1: SSG 20 Ports and Power Connectors**

Port	Description	Connector	Speed/Protocol
0/0-0/4	Enables direct connections to workstations or a LAN connection through a switch or hub. This connection also allows you to manage the device through a Telnet session or the WebUI.	RJ-45	10/100 Mbps Ethernet Autosensing duplex and auto MDI/MDIX
USB	Enables a 1.1 USB connection with the system.	N/A	12M (full speed) or 1.5M (low speed)
Console	Enables a serial connection with the system. Used for terminal-emulation connectivity to launch CLI sessions.	RJ-45	9600 bps/RS-232C serial
AUX	Enables a backup RS-232 async serial Internet connection through an external modem.	RJ-45	9600 bps — 115 Kbps/RS-232C serial
Mini PIM			
ADSL 2/2 +	Enables an Internet connection through an ADSL data link.	RJ-11 (Annex A) RJ-45 (Annex B)	ANSI T1.413 Issue 2 (Annex A only) ITU G.992.1 (G.dmt) ITU G.992.3 (ADSL2) ITU G.992.5 (ADSL2 +)
V.92 Modem	Enables a primary or backup Internet or untrusted network connection to a service provider.	RJ-11	9600 bps — 115 Kbps/RS-232 serial autosensing duplex and polarity
T1	Enables a connection to the T1 line to the untrusted network.	RJ-45	1.544 Mbps (full-time slots)
E1	Enables a connection to the E1 line to the untrusted network.	RJ-45	2.048 Mbps (full-time slots)
ISDN	Enables the ISDN line to be used as the untrust or backup interface. (S/T)	RJ-45	B-channels at 64 Kbps Leased line at 128 Kbps
Antenna A & B (SSG 20-WLAN)	Enables a direct connection to workstations in the vicinity of a wireless radio connection.	RPSMA	802.11a (54 Mbps on 5GHz radio band) 802.11b (11 Mbps on 2.4 GHz radio band) 802.11g (54 Mbps on 2.4 GHz radio band) 802.11 superG (108 Mbps on 2.4 GHz and 5GHz radio bands)

## Front Panel

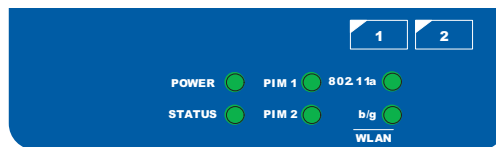
This section describes the following elements on the front panel of an SSG 20 device:

- System Status LEDs
- Port Descriptions
- Mini Physical Interface Module Port Descriptions

### System Status LEDs

The system status LEDs display information about critical device functions. Figure 3 illustrates the position of each status LED on the front of the SSG 20-WLAN device. The WLAN LEDs are only present on the SSG 20-WLAN device.

**Figure 3: Status LEDs**



When the system powers up, the POWER LED changes from off to blinking green, and the STATUS LED changes in the following sequence: red, green, blinking green. Startup takes approximately two minutes to complete. If you want to turn the system off and on again, we recommend you wait a few seconds between shutting it down and powering it back up. Table 2 provides the name, color, status, and description of each system status LED.

**Table 2: Status LED Descriptions**

Name	Color	Status	Description
POWER	Green	On steadily	Indicates that the system is receiving power.
		Off	Indicates that the system is not receiving power.
	Red	On steadily	Indicates that the device is not operating normally.
		Off	Indicates that the device is operating normally.
STATUS	Green	On steadily	Indicates that the system is starting or performing diagnostics.
		Blinking	Indicates that the device is operating normally.
	Red	Blinking	Indicates that there is an error detected.
PIM 1	Green	On steadily	Indicates that the mini PIM is functioning.
		Blinking	Indicates that the mini PIM is passing traffic.
		Off	Indicates that the mini PIM is not operational.

<b>Name</b>	<b>Color</b>	<b>Status</b>	<b>Description</b>
PIM 2	Green	On steadily	Indicates that the mini PIM is functioning.
		Blinking	Indicates that the mini PIM is passing traffic.
		Off	Indicates that the mini PIM is not operational.
WLAN (On WLAN device only)			
802.11a	Green	On steadily	Indicates that a wireless connection is established but there is no link activity.
		Blinking slowly	Indicates that a wireless connection is established. The baud rate is proportional to the link activity.
		Off	Indicates that there is no wireless connection established.
b/g	Green	On steadily	Indicates that a wireless connection is established but there is no link activity.
		Blinking slowly	Indicates that a wireless connection is established. The baud rate is proportional to the link activity.
		Off	Indicates that there is no wireless connection established.

## Port Descriptions

This section explains the purpose and function of the following:

- Ethernet Ports
- Console Port
- AUX Port

### Ethernet Ports

Five 10/100 Ethernet ports provide LAN connections to hubs, switches, local servers, and workstations. You can also designate an Ethernet port for management traffic. The ports are labeled **0/0** through **0/4**. For the default zone bindings for each Ethernet port, see “Default Device Settings” on page 31.

When configuring one of the ports, reference the interface name that corresponds to the location of the port. From left to right on the front panel, the interface names for the ports are **ethernet0/0** through **ethernet0/4**.

Figure 4 displays the location of the LEDs on each Ethernet port.

**Figure 4: Activity Link LEDs Location**

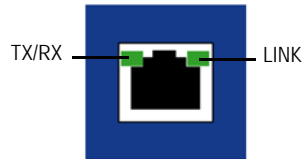


Table 3 describes the Ethernet port LEDs.

**Table 3: LAN Port LEDs**

Name	Color	Status	Description
LINK	Green	On steadily	Port is online.
		Off	Port is offline.
TX/RX	Green	Blinking	Traffic is passing through. The baud rate is proportional to the link activity.
		Off	Port might be on but is not receiving data.

### Console Port

The Console port is an RJ-45 serial port wired as data circuit-terminating equipment (DCE) that can be used for local administration. Use a straight-through cable when using a terminal connection and a crossover cable when connecting to another DCE device. An RJ-45 to DB-9 adapter is supplied.

See “Connectors” on page 60 for the RJ-45 connector pinouts.

### AUX Port

The auxiliary (AUX) port is an RJ-45 serial port wired as data terminal equipment (DTE) that can be connected to a modem to allow remote administration. We do not recommend using this port for regular remote administration. The AUX port is typically assigned to be the backup serial interface. The baud rate is adjustable from 9600 bps to 115200 bps and requires hardware flow control. Use a straight-through cable when connecting to a modem and a crossover cable when connecting to another DTE device.

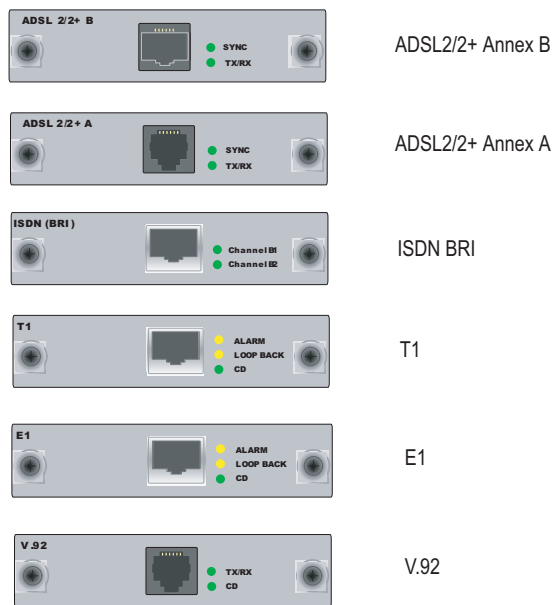
See “Connectors” on page 60 for the RJ-45 connector pinouts.

### Mini Physical Interface Module Port Descriptions

Each mini physical interface module (PIM) supported on a device has the following components:

- One cable connector port—Accepts a network media connector. Figure 5 shows the available mini PIMs. You can install up to two mini PIMs in a device.

**Figure 5: Mini PIMs for the SSG 20**



- Two to three status LEDs—Indicate port status. Table 4 describes the meaning of the LED states.

**Table 4: Mini PIM LED States on the SSG 20**

Type	Name	Color	State	Description
ADSL 2/2 + (Annex A and B)	SYNC	Green	On steadily	Indicates that the ADSL interface is trained
			Blinking	Indicates training is in progress
			Off	Indicates that the interface is idle
	TX/RX	Green	Blinking	Indicates that traffic is passing through
			Off	Indicates that no traffic is passing through
	ISDN (BRI)	CH B1	Green	On steadily
Off				Indicates that B-Channel 1 is not active
CH B2		Green	On steadily	Indicates that B-Channel 2 is active
			Off	Indicates that B-Channel 2 is not active
T1/E1	ALARM	Yellow	On steadily	Indicates that there is a local or remote alarm; device has detected a failure
			Off	Indicates that there are no alarms or failures
	LOOP BACK	Yellow	On steadily	Indicates that a loopback or line state is detected
			Off	Indicates that the loopback is not active
	CD	Green	On steadily	Indicates a carrier was detected and the internal DSU/CSU in the mini PIM is communicating with another DSU/CSU
			Off	Indicates that carrier detect is not active
V.92	CD	Green	On steadily	Indicates that the link is active
			Off	Indicates that the serial interface is not in service
	TX/RX	Green	Blinking	Indicates that traffic is passing through
			Off	Indicates that no traffic is passing through



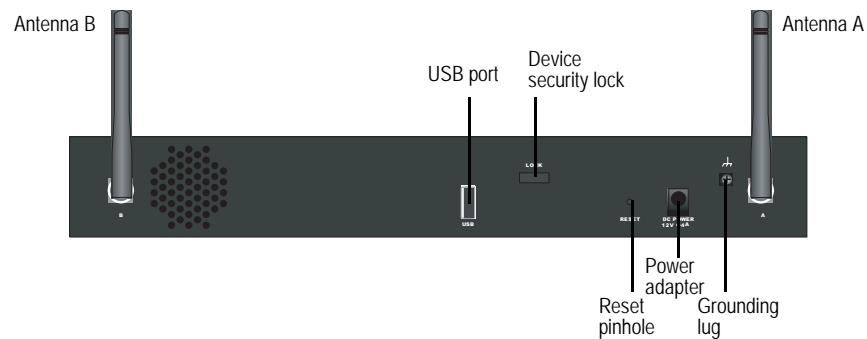
**CAUTION:** Mini PIMs are not hot-swappable. You must install them in the front panel slots before powering on the device.

## Back Panel

This section describes the following elements on the back panel of an SSG 20 device:

- Power Adapter
- Radio Transceivers
- Grounding Lug
- Antennae Types
- USB Port

**Figure 6: Back Panel of an SSG 20-WLAN Device**



### Power Adapter

The POWER LED on the front panel of a device either glows green or is off. Green indicates correct function, and off indicates power-adapter failure or that the device is off.

### Radio Transceivers

The SSG 20-WLAN contains two wireless connectivity radio transceivers, which support 802.11a/b/g standards. The first transceiver (WLAN 0) uses the 2.4 GHz radio band, which supports the 802.11b standard at 11 Mbps, the 802.11g standard at 54 Mbps, and 802.11 SuperG standard at 108 Mbps. The second radio transceiver (WLAN 1) uses the 5GHz radio band, which supports the 802.11a standard at 54 Mbps. For information on configuring the wireless radio band, see “This section provides information for configuring the wireless interface on the SSG 20-WLAN device. Wireless networks consist of names referred to as Service Set Identifiers (SSIDs). Specifying SSIDs allows you to have multiple wireless networks reside in the same location without interfering with each other. An SSID name can have a maximum of 32 characters. If a space is part of the SSID name string, then the string must be enclosed with quotation marks. Once the SSID name is set, more SSID attributes can be configured. To use the wireless local area network (WLAN) capabilities on the device, you must configure at least one SSID and bind it to a wireless interface.” on page 37.



## **Grounding Lug**

A one-hole grounding lug is provided on the rear of the chassis to connect the device to earth ground (see Figure 6).

To ground the device before connecting power, connect a grounding cable to earth ground and then attach the cable to the lug on the rear of the chassis.

## Antennae Types

The SSG 20-WLAN device supports three types of custom-built radio antennae:

- **Diversity antennae** — The diversity antennae provide 2dBi directional coverage and a fairly uniform level of signal strength within the area of coverage and are suitable for most installations. This type of antennae is shipped with the device.
- **External omnidirectional antenna** — The external antenna provides 2dBi omnidirectional coverage. Unlike diversity antennae, which function as a pair, an external antenna operates to eliminate an echo effect that can sometimes occur from slightly delayed characteristics in signal reception when two are in use.
- **External directional antenna** — The external directional antenna provides 2dBi unidirectional coverage and is appropriate for locations like hallways and outer walls (with the antenna facing inward).

## USB Port

The USB port on the back panel of an SSG 20 device accepts a universal serial bus (USB) storage device or USB storage device adapter with a compact-flash disk installed, as defined in the *CompactFlash Specification* published by the CompactFlash Association. When the USB storage device is installed and configured, it automatically acts as a secondary boot device if the primary compact-flash disk fails on startup.

The USB port allows file transfers such as device configurations, user certifications, and update version images between an external USB storage device and the internal flash storage located in the security device. The USB port supports USB 1.1 specification at either low speed (1.5M) or full speed (12M) file transfer.

To transfer files between the USB storage device and an SSG 20, perform the following steps:

1. Insert the USB storage device into the USB port on the security device.
2. Save the files from the USB storage device to the internal flash storage on the device with the **save {software | config | image-key} from usb filename to flash** CLI command.
3. Before removing the USB storage device, stop the USB port with the **exec usb-device stop** CLI command.
4. It is now safe to remove the USB storage device.

If you want to delete a file from the USB storage device, use the **delete file usb:filename** CLI command.

If you want to view the saved file information on the USB storage device or internal flash storage, use the **get file** CLI command.

## Chapter 2

# Installing and Connecting the Device

This chapter describes how to mount an SSG 20 device and connect cables and power to the device. This chapter contains the following sections:

- “Before You Begin” on page 20
- “Installing Equipment” on page 20
- “Connecting Interface Cables to a Device” on page 22
- “Connecting the Power” on page 22
- “Connecting a Device to a Network” on page 23

---

**NOTE:** For safety warnings and instructions, refer to the *Juniper Networks Security Products Safety Guide*. Before working on any equipment, you should be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

---

## Before You Begin

---

The location of the chassis, the layout of the mounting equipment, and the security of your wiring room are crucial for proper system operation.



---

**WARNING:** To prevent abuse and intrusion by unauthorized personnel, install the SSG 20 device in a secure environment.

---

Observing the following precautions can prevent shutdowns, equipment failures, and injuries:

- Before installation, always check that the power supply is disconnected from any power source.
- Ensure that the room in which you operate the device has adequate air circulation and that the room temperature does not exceed 104°F (40°C).
- Do not place the device in an equipment-rack frame that blocks an intake or exhaust port. Ensure that enclosed racks have fans and louvered sides.
- Correct these hazardous conditions before any installation: moist or wet floors, leaks, ungrounded or frayed power cables, or missing safety grounds.

## Installing Equipment

---

You can front-mount, wall-mount, or desk-mount an SSG 20 device. The mounting kits may be purchased separately.

To mount an SSG 20 device, you need a number-2 phillips screwdriver (not provided) and screws that are compatible with the equipment rack (included in the kit).

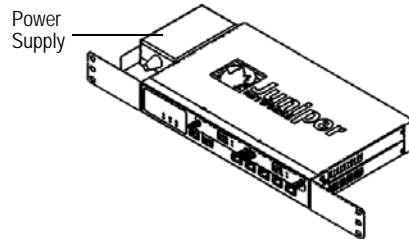
---

**NOTE:** When mounting a device, make sure that it is within reach of the power outlet.

---

To front-mount an SSG 20 device onto a standard 19-inch equipment rack, perform the following steps:

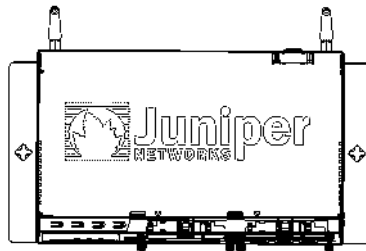
**Figure 7: SSG 20 Front-mount**



1. Align the power supply rack-mount ear to the left-front edge of the device.
2. Place the screws in the holes and use a phillips screwdriver to secure them.
3. Align the other rack-mount ear to the right-front edge of the device.
4. Place the screws in the holes and use a phillips screwdriver to secure them.
5. Mount the device on the rack with the provided screws.
6. Plug the power supply into the power outlet.

To wall-mount an SSG 20 device, perform the following steps:

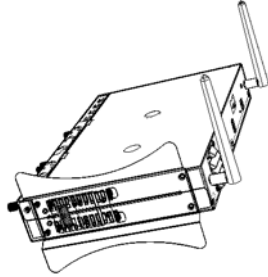
**Figure 8: SSG 20 Wall-mount**



1. Align the wall-mount ears to the device.
2. Place the screws in the holes and use a phillips screwdriver to secure them.
3. Ensure that the wall to be used is smooth, flat, dry, and sturdy.
4. Mount the device on the wall using the provided screws.
5. Plug the power supply into the power outlet.

To desk-mount an SSG 20 device, perform the following steps:

**Figure 9: SSG 20 Desk-mount**



1. Attach the desktop stand to the side of the device. We recommend using the side closest to the power adapter.
2. Place the mounted device on the desktop.
3. Plug in the power adapter and connect the power supply to the power outlet.

## Connecting Interface Cables to a Device

---

To connect the interface cable to a device, perform the following steps:

1. Have ready a length of the type of cable used by the interface.
2. Insert the cable connector into the cable-connector port on the interface faceplate.
3. Arrange the cable as follows to prevent it from dislodging or developing stress points:
  - a. Secure the cable so that it is not supporting its own weight as it hangs to the floor.
  - b. Place any excess cable out of the way in a neatly coiled loop.
  - c. Use fasteners to maintain the shape of the cable loops.

## Connecting the Power

---

To connect the power to a device, perform the following steps:

1. Plug the DC-connector end of the power cable into the DC-power receptacle on the back of the device.
2. Plug the AC-adapter end of the power cable into an AC-power source.



**WARNING:** We recommend using a surge protector for the power connection.

---

## Connecting a Device to a Network

---

An SSG 20 device provides firewall and general security for networks when it is placed between internal networks and the untrusted network. This section describes the following:

- Connecting a Device to an Untrusted Network
- Connecting a Device to an Internal Network or a Workstation

### Connecting a Device to an Untrusted Network

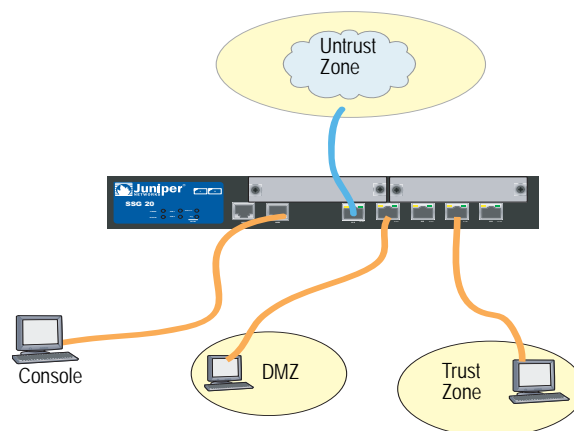
You can connect your SSG 20 device to an untrusted network in one of the following ways:

- Ethernet Ports
- Serial (AUX/Console) Ports
- Connecting Mini PIMs to an Untrusted Network

Figure 10 shows the SSG 20 with basic network cabling connections with two blank mini-PIMs and the 10/100 Ethernet ports cabled as follows:

- The port labeled 0/0 (ethernet0/0 interface) is connected to the untrust network.
- The port labeled 0/1 (ethernet0/1 interface) is connected to a workstation in the DMZ security zone.
- The port labeled 0/3 (brgoup0 interface) is connected to a workstation in the Trust security zone.
- The Console port is connected to a serial terminal for management access.

**Figure 10: Basic Networking Example**



## Ethernet Ports

To establish a high-speed connection, connect the provided Ethernet cable from the Ethernet port marked 0/0 on an SSG 20 device to the external router. The device autosenses the correct speed, duplex, and MDI/MDIX settings.

## Serial (AUX/Console) Ports

You can connect to the untrusted network with an RJ-45 straight-through serial cable and an external modem.



**WARNING:** Make sure that you do not inadvertently connect the Console, AUX, or Ethernet ports on the device to the telephone outlet.

---

## Connecting Mini PIMs to an Untrusted Network

This section explains how to connect the device mini PIMs to an untrusted network.

### ADSL2/2+ Mini PIM

Connect the provided ADSL cable from the ADSL2/2+ mini PIM to your telephone outlet. The ADSL port on the Annex A version of the device uses an RJ-11 connector, while the Annex B version uses an RJ-45 connector. In the case of Annex B models, the cable you connect from the ADSL port to the telephone outlet is identical in appearance and wiring to a straight-through 10 Base-T Ethernet cable.

### Connecting Splitters and Microfilters

A *signal splitter* divides the telephone signal into low-frequency voice signals for voice calls and high-frequency data signals for data traffic. Your service provider usually installs the splitter as part of the equipment that connects your site telephone lines to the provider network.

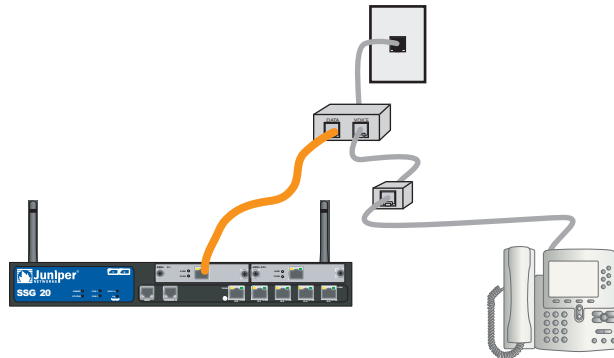
There are also splitters that you may be able to install yourself, depending upon your service-provider equipment. If you are installing such a splitter yourself, connect the ADSL cable from the device and the telephone line to the appropriate connectors (for example, “data” or “voice”) on the splitter. You connect the other end of the splitter to the telephone outlet.

You may need to install a *microfilter* on each telephone, fax machine, answering machine, or analog modem that connects to the ADSL line. The microfilter filters out high-frequency noise on the telephone line. You install the microfilter on the telephone line between the telephone, fax machine, answering machine, or analog modem and the voice connector on the splitter.

Figure 11 shows an example of a microfilter and a splitter that you install on your site. (You must obtain the appropriate microfilters or splitters from your service provider.)



**Figure 11: Microfilter and Splitter on Your Network Connection**



### **ISDN, T1, E1, and V.92 Mini PIMs**

To connect the mini PIMs to a device, perform the following steps:

1. Have ready a length of the type of cable used by the interface.
2. Insert the cable connector into the cable-connector port on the interface faceplate.
3. Arrange the cable as follows to prevent it from dislodging or developing stress points:
  - a. Secure the cable so that it is not supporting its own weight as it hangs to the floor.
  - b. Place any excess cable out of the way in a neatly coiled loop.
  - c. Use fasteners to maintain the shape of the cable loops.

To configure the ISDN, E1, T1, or V.92 mini PIM, see “Mini PIM Configuration” on page 41.

### **Connecting a Device to an Internal Network or a Workstation**

You can connect your local area network (LAN) or workstation with the Ethernet and/or wireless interfaces.

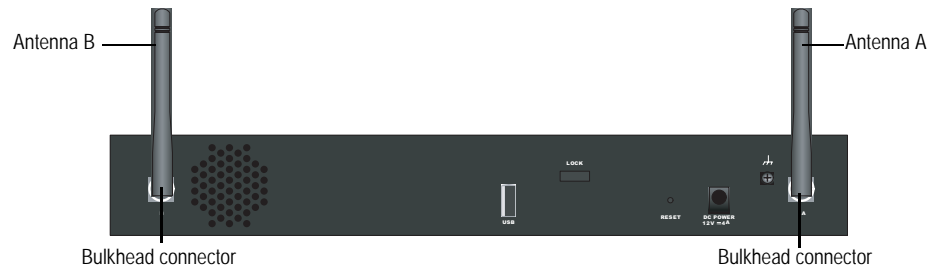
#### **Ethernet Ports**

An SSG 20 device contains five Ethernet ports. You can use one or more of these ports to connect to LANs through switches or hubs. You can also connect one or all of the ports directly to workstations, eliminating the need for a hub or switch. You can use either crossover or straight-through cables to connect the Ethernet ports to other devices. See “Default Device Settings” on page 31 for the default zone-to-interface bindings.

## Wireless Antennae

If you are using the wireless interface, you need to connect the provided antennae on the device. If you have the standard 2dB diversity antennae, use screws to attach them onto the posts marked A and B at the back of the device. Bend each antenna at its elbows, making sure not to put pressure on the bulkhead connectors.

**Figure 12: SSG 20-WLAN Antennae Location**



If you are using the optional external antenna, follow the connection instructions that came with that antenna.

## Chapter 3

# Configuring the Device

ScreenOS software is preinstalled on an SSG 20 device. When the device is powered on, it is ready to be configured. While the device has a default factory configuration that allows you to initially connect to the device, you need to perform further configuration for your specific network requirements.

This chapter contains the following sections:

- “Accessing a Device” on page 28
- “Default Device Settings” on page 31
- “Basic Device Configuration” on page 33
- “Basic Wireless Configuration” on page 37
- “Mini PIM Configuration” on page 41
- “Basic Firewall Protections” on page 48
- “Verifying External Connectivity” on page 48
- “Resetting a Device to Factory Defaults” on page 49

---

**NOTE:** After you configure a device and verify connectivity through the remote network, you must register your product at [www.juniper.net/support/](http://www.juniper.net/support/) so certain ScreenOS services, such as Deep Inspection Signature Service and Antivirus (purchased separately), can be activated on the device. After registering your product, use the WebUI to obtain the subscription for the service. For more information about registering your product and obtaining subscriptions for specific services, refer to the *Fundamentals* volume of the *Concepts & Examples ScreenOS Reference Guide* for the ScreenOS version running on the device.

---

## Accessing a Device

You can configure and manage a device in several ways:

- **Console:** The Console port on the device allows you to access the device through a serial cable connected to your workstation or terminal. To configure the device, you enter ScreenOS command line interface (CLI) commands on your terminal or in a terminal-emulation program on your workstation.
- **WebUI:** The ScreenOS Web User Interface (WebUI) is a graphical interface available through a browser. To initially use the WebUI, the workstation on which you run the browser must be on the same subnetwork as the device. You can also access the WebUI through a secure server using Secure Sockets Layer (SSL) with secure HTTP (S-HTTP).
- **Telnet/SSH:** Telnet and SSH are applications that allows you to access devices through an IP network. To configure the device, you enter ScreenOS CLI commands in a Telnet session from your workstation. For more information, refer to the *Administration* volume of the *Concepts & Examples ScreenOS Reference Guide*.
- **NetScreen-Security Manager:** NetScreen-Security Manager is a Juniper Networks enterprise-level management application that enables you to control and manage Juniper Networks firewall/IPSec VPN devices. For instructions on how to manage your device with NetScreen-Security Manager, refer to the *NetScreen-Security Manager Administrator's Guide*.

## Using a Console Connection

**NOTE:** Use a straight-through RJ-45 CAT5 serial cable with a male RJ-45 connector to plug into the Console port on the device.

To establish a console connection, perform the following steps:

1. Plug the female end of the supplied DB-9 adapter into the serial port of your workstation. (Be sure that the DB-9 is inserted properly and secured.) Figure 13 shows the type of DB-9 connector that is needed.

**Figure 13: DB-9 Adapter**



2. Plug the male end of the RJ-45 CAT5 serial cable into the Console port on the SSG 20. (Be sure that the other end of the CAT5 cable is inserted properly and secured in the DB-9 adapter.)

3. Launch a serial terminal-emulation program on your workstation. The required settings to launch a console session are as follows:
  - Baud rate: 9600
  - Parity: None
  - Data bits: 8
  - Stop bit: 1
  - Flow Control: None
4. If you have not yet changed the default login for the admin name and password, enter **netscreen** at both the login and password prompts. (Use lowercase letters only. The login and password fields are both case-sensitive.)

For information on how to configure the device with the CLI commands, refer to the *Concepts & Examples ScreenOS Reference Guide*.
5. (Optional) By default, the console times out and terminates automatically after 10 minutes of idle time. To remove the timeout, enter **set console timeout 0**.

## Using the WebUI

To use the WebUI, the workstation from which you are managing the device must initially be on the same subnetwork as the device. To access the device with the WebUI, perform the following steps:

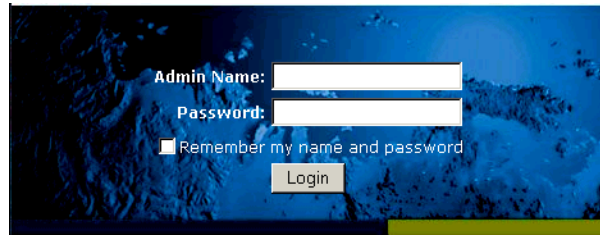
1. Connect your workstation to the 0/2 — 0/4 port (bgroup0 interface in the Trust zone) on the device.
2. Ensure that your workstation is configured for Dynamic Host Configuration Protocol (DHCP) or is statically configured with an IP address in the 192.168.1.0/24 subnet.
3. Launch your browser, enter the IP address for the bgroup0 interface (the default IP address is 192.168.1.1/24), then press **Enter**.

---

**NOTE:** When the device is accessed through the WebUI the first time, the Initial Configuration Wizard (ICW) appears. If you decide to use the ICW to configure your device, see “Initial Configuration Wizard” on page 63.

---

The WebUI application displays the login prompt as shown in Figure 14.

**Figure 14: WebUI Login Prompt**

4. If you have not yet changed the default login for the admin name and password, enter **netscreen** at both the admin name and password prompts. (Use lowercase letters only. The login and password fields are both case-sensitive.)

## Using Telnet

To establish a Telnet connection, perform the following steps:

1. Connect your workstation to the 0/2 — 0/4 port (bgroup0 interface in the Trust zone) on the device.
2. Ensure that your workstation is configured for DHCP or is statically configured with an IP address in the 192.168.1.0/24 subnet.
3. Start a Telnet client application to the IP address for the bgroup0 interface (the default IP address is 192.168.1.1). For example, enter **telnet 192.168.1.1**.

The Telnet application displays the login prompt.

4. If you have not yet changed the default login for the login and password, enter **netscreen** at both the login and password prompts. (Use lowercase letters only. The login and password fields are both case-sensitive.)
5. (Optional) By default, the console times out and terminates automatically after 10 minutes of idle time. To remove the timeout, enter **set console timeout 0**.

## Default Device Settings

This section describes the default settings and operation of an SSG 20 device.

Table 5 shows the default zone bindings for ports on the devices.

**Table 5: Default Physical Interface to Zone Bindings**

Port Label	Interface	Zone
<b>10/100 Ethernet ports:</b>		
0/0	ethernet0/0	Untrust
0/1	ethernet0/1	DMZ
0/2	bgroup0 (ethernet0/2)	Trust
0/3	bgroup0 (ethernet0/3)	Trust
0/4	bgroup0 (ethernet0/4)	Trust
AUX	serial0/0	Null
<b>WAN mini PIM ports (x = mini PIM slot 1 or 2):</b>		
ADSL2/2 + (Annex A)	adsl(x/0)	Untrust
ADSL2/2 + (Annex B)	adsl(x/0)	Untrust
T1	serial(x/0)	Untrust
E1	serial(x/0)	Untrust
ISDN	bri(x/0)	Untrust
V.92	serial(x/0)	Null

A bridge group (bgroup) is designed to allow network users to switch between wired and wireless traffic without having to reconfigure or reboot the device. By default, the ethernet0/2 — ethernet0/4 interfaces, labeled as ports 0/2 — 0/4 on the device, are grouped together as the bgroup0 interface, have the IP address 192.168.1.1/24, and are bound to the Trust security zone. You can configure up to four bgroups.

If you want to set an Ethernet or a wireless interface into a bgroup, you must first make sure that the Ethernet or wireless interface is in the Null security zone. Unsetting the Ethernet or wireless interface that is in a bgroup places the interface in the Null security zone. Once assigned to the Null security zone, the Ethernet interface can be bound to a security zone and assigned a different IP address.

To unset ethernet0/3 from bgroup0 and assign it to the Trust zone with a static IP address of 192.168.3.1/24, use the WebUI or CLI as follows:

**WebUI**

Network > Interfaces > List > Edit (bgroup0) > Bind Port: deselect **ethernet0/3**, then click **Apply**.

List > Edit (ethernet0/3): Enter the following, then click **Apply**:

Zone Name: Trust (select)  
 IP Address/Netmask: 192.168.3.1/24

**CLI**

```
unset interface bgroup0 port ethernet0/3
set interface ethernet0/3 zone trust
set interface ethernet0/3 ip 192.168.3.1/24
save
```

**Table 6: Wireless and Logical Interface Bindings**

SSG 20-WLAN	Interface	Zone
<b>Wireless Interface</b> Specifies a wireless interface, which is configurable to operate on 2.4G and/or 5G radio	wireless0/0 (default IP address is 192.168.2.1/24).	Trust
	wireless0/1-0/3.	Null
<b>Logical Interfaces</b>		
Layer-2 interface	vlan1 specifies the logical interfaces used for management and VPN traffic termination while the device is in Transparent mode.	N/A
Tunnel interfaces	tunnel.n specifies a logical tunnel interface. This interface is for VPN traffic.	N/A

You can change the default IP address on the bgroup0 interface to match the addresses on your LAN and WLAN. For configuring a wireless interface to a bgroup, see “Basic Wireless Configuration” on page 37.

---

**NOTE:** The bgroup interface does not work in Transparent mode when it contains a wireless interface.

---

For additional bgroup information and examples, refer to the *Concepts & Examples ScreenOS Reference Guide*.

There are no other default IP addresses configured on other Ethernet or wireless interfaces on a device; you need to assign IP addresses to the other interfaces, including the WAN interfaces.



## Basic Device Configuration

---

This section describes the following basic configuration settings:

- Root Admin Name and Password
- Date and Time
- Bridge Group Interfaces
- Administrative Access
- Management Services
- Hostname and Domain Name
- Default Route
- Management Interface Address
- Backup Untrust Interface Configuration

### Root Admin Name and Password

The root admin user has complete privileges for configuring an SSG 20 device. We recommend that you change the default root admin name and password (both **netscreen**) immediately.

To change the root admin name and password, use the WebUI or CLI as follows:

#### WebUI

Configuration > Admin > Administrators > Edit (for the netscreen administrator name value): Enter the following, then click **OK**:

Administrator Name:  
Old Password: netscreen  
New Password:  
Confirm New Password:

---

**NOTE:** Passwords are not displayed in the WebUI.

---

#### CLI

```
set admin name name
set admin password pswd_str
save
```

## Date and Time

The time set on an SSG 20 device affects events such as the setup of VPN tunnels. The easiest way to set the date and time on the device is to use the WebUI to synchronize the device system clock with the workstation clock.

To configure the date and time on a device, use the WebUI or CLI as follows:

### WebUI

1. Configuration > Date/Time: Click the Sync Clock with Client button.

A pop-up message prompts you to specify if you have enabled the daylight saving time option on your workstation clock.

2. Click **Yes** to synchronize the system clock and adjust it according to daylight saving time, or click **No** to synchronize the system clock without adjusting for daylight saving time.

You can also use the **set clock** CLI command in a Telnet or Console session to manually enter the date and time for the device.

## Bridge Group Interfaces

By default, the SSG 20 device has Ethernet interfaces ethernet0/2 — ethernet0/4 grouped together in the Trust security zone. Grouping interfaces sets interfaces in one subnet. You can unset an interface from a group and assign it to a different security zone. Interfaces must be in the Null security zone before they can be assigned to a group. To place a grouped interface in the Null security zone, use the **unset interface interface port interface** CLI command.

The SSG 20-WLAN devices allow Ethernet and wireless interfaces to be grouped under one subnet.

---

**NOTE:** Only wireless and Ethernet interfaces can be set in a bgroup.

---

To configure a group with Ethernet and wireless interfaces, use the WebUI or CLI as follows:

### WebUI

Network > Interfaces > List > Edit (bgroup0) > Bind Port: deselect **ethernet0/3** and **ethernet0/4**, then click **Apply**.

Edit (bgroup1) > Bind Port: select **ethernet0/3**, **ethernet0/4**, and **wireless0/2**, then click **Apply**.

> Basic: Enter the following, then click **Apply**:

Zone Name: DMZ (select)  
IP Address/Netmask: 10.0.0.1/24

### **CLI**

```
unset interface bgroup0 port ethernet0/3
unset interface bgroup0 port ethernet0/4
set interface bgroup1 port ethernet0/3
set interface bgroup1 port ethernet0/4
set interface bgroup1 port wireless0/2
set interface bgroup1 zone DMZ
set interface bgroup1 ip 10.0.0.1/24
save
```

## **Administrative Access**

By default, anyone in your network can manage a device if they know the login and password.

To configure the device to be managed only from a specific host on your network, use the WebUI or CLI as follows:

### **WebUI**

Configuration > Admin > Permitted IPs: Enter the following, then click **Add**:

IP Address/Netmask: *ip\_addr/mask*

### **CLI**

```
set admin manager-ip ip_addr/mask
save
```

## **Management Services**

ScreenOS provides services for configuring and managing the device, such as SNMP, SSL, and SSH, which you can enable on a per-interface basis.

To configure the management services on the device, use the WebUI or CLI as follows:

### **WebUI**

Network > Interfaces > List > Edit (for ethernet0/0): Under **Management Services**, select or clear the management services you want to use on the interface, then click **Apply**.

### **CLI**

```
set interface ethernet0/0 manage web
unset interface ethernet0/0 manage snmp
save
```

## Hostname and Domain Name

The domain name defines the network or subnetwork that the device belongs to, while the hostname refers to a specific device. The hostname and domain name together uniquely identify the device in the network.

To configure the hostname and domain name on a device, use the WebUI or CLI as follows:

### WebUI

Network > DNS > Host: Enter the following, then click **Apply**:

Host Name: *name*  
Domain Name: *name*

### CLI

```
set hostname name
set domain name
save
```

## Default Route

The default route is a static route used to direct packets addressed to networks that are not explicitly listed in the routing table. If a packet arrives at the device with an address for which the device does not have routing information, the device sends the packet to the destination specified by the default route.

To configure the default route on the device, use the WebUI or CLI as follows:

### WebUI

Network > Routing > Destination > New (trust-vr): Enter the following, then click **OK**:

IP Address/Netmask: 0.0.0.0/0.0.0.0  
Next Hop  
Gateway: (select)  
Interface: ethernet0/2 (select)  
Gateway IP Address: *ip\_addr*

### CLI

```
set route 0.0.0.0/0 interface ethernet0/2 gateway ip_addr
save
```

## Management Interface Address

The Trust interface has the default IP address 192.168.1.1/24 and is configured for management services. If you connect the 0/2 — 0/4 ports on the device to a workstation, you can configure the device from a workstation in the 192.168.1.1/24 subnetwork using a management service such as Telnet.

You can change the default IP address on the Trust interface. For example, you might want to change the interface to match IP addresses that already exist on your LAN.

## Backup Untrust Interface Configuration

The SSG 20 device allows you to configure a backup interface for untrust failover. To set a backup interface for untrust failover, perform the following steps:

1. Set the backup interface in the Null security zone with the **unset interface interface [port interface]** CLI command.
2. Bind the backup interface to the same security zone as the primary interface with the **set interface interface zone zone\_name** CLI command.

---

**NOTE:** The primary and backup interfaces must be in the same security zone. One primary interface has only one backup interface, and one backup interface has only one primary interface.

---

To set the ethernet0/4 interface as the backup interface to the ethernet0/0 interface, use the WebUI or CLI as follows:

### WebUI

Network > Interfaces > Backup > Enter the following, then click **Apply**.

Primary: ethernet0/0  
Backup: ethernet0/4  
Type: track-ip (select)

### CLI

```
unset interface bgroup0 port ethernet0/4
set interface ethernet0/4 zone untrust
set interface ethernet0/0 backup interface ethernet0/4 type track-ip
save
```

## Basic Wireless Configuration

---

This section provides information for configuring the wireless interface on the SSG 20-WLAN device. Wireless networks consist of names referred to as Service Set Identifiers (SSIDs). Specifying SSIDs allows you to have multiple wireless networks reside in the same location without interfering with each other. An SSID name can have a maximum of 32 characters. If a space is part of the SSID name string, then the string must be enclosed with quotation marks. Once the SSID name is set, more SSID attributes can be configured. To use the wireless local area network (WLAN) capabilities on the device, you must configure at least one SSID and bind it to a wireless interface.

The SSG 20-WLAN device allows you to create up to 16 SSIDs, but only 4 of them can be used simultaneously. You can configure the device to use the 4 SSIDs on either one of the transceivers or split the use on both (for example, 3 SSIDs assigned to WLAN 0 and 1 SSID assigned to WLAN 1.) Use the **set interface wireless\_interface wlan {0 | 1 | both}** CLI command to set the radio transceivers on the SSG 20-WLAN device.

Once you have set an SSID to the wireless0/0 interface, you can access the device using the default wireless0/0 interface IP address in the steps described in “Accessing a Device” on page 28. Figure 15 shows the default configuration for the SSG 20-WLAN device.

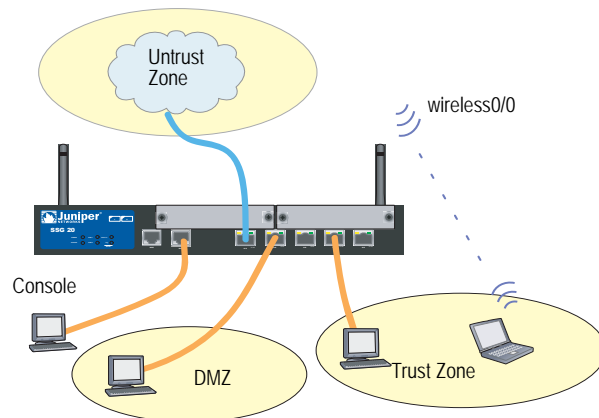
---

**NOTE:** If you are operating the SSG 20-WLAN device in a country other than the United States, Japan, Canada, China, Taiwan, Korea, Israel, or Singapore, then you must use the **set wlan country-code** CLI command or set it on the Wireless > General Settings WebUI page before a WLAN connection can be established. This command sets the selectable channel range and the transmit power level.

If your regional code is ETSI, you must set the correct country code that meets your local radio spectrum regulations.

---

**Figure 15: Default SSG 20-WLAN Configuration**



By default, the wireless0/0 interface is configured with the IP address 192.168.2.1/24. All wireless clients that need to connect to the Trust zone must have an IP address in the wireless subnetwork. You can also configure the device to use DHCP to automatically assign IP addresses in the 192.168.2.1/24 subnetwork to your devices.

By default, the wireless0/1 – wireless0/3 interfaces are defined as Null and do not have IP addresses assigned to them. If you want to use any of the other wireless interfaces, you must configure an IP address for it, assign an SSID to it, and bind it to a security zone. Table 7 displays the wireless authentication and encryption methods.

**Table 7: Wireless Authentication and Encryption Options**

Authentication	Encryption
Open	Allows any wireless client to access the device
Shared-key	WEP shared-key
WPA-PSK	AES/TKIP with pre-shared key
WPA	AES/TKIP with key from RADIUS server
WPA2-PSK	802.11i compliant with a pre-shared key
WPA2	802.11i compliant with a RADIUS server
WPA-Auto-PSK	Allows WPA and WPA2 type with pre-shared key
WPA-Auto	Allows WPA and WPA2 type with RADIUS server
802.1x	WEP with key from RADIUS server

Refer to the *Concepts & Examples ScreenOS Reference Guide* for configuration examples, SSID attributes, and CLI commands relating to wireless security configurations.

To configure a wireless interface for basic connectivity, use the WebUI or CLI as follows:

**WebUI**

1. Set the WLAN country code and IP address.

Wireless > General Settings > Select the following, then click **Apply**:

Country code: Select your code  
IP Address/Netmask: *ip\_add/netmask*

2. Set the SSID.

Wireless > SSID > New: Enter the following, then click **OK**:

SSID:  
Authentication:  
Encryption:  
Wireless Interface Binding:

3. (Optional) set the WEP key.

SSID > WEP Keys: Select the keyID, then click **Apply**.

4. Set the WLAN mode.

Network > Interfaces > List > Edit (wireless interface): Select **Both** for the WLAN mode, then click **Apply**.

5. Activate wireless changes.

Wireless > General Settings > Click **Activate Changes**.

### CLI

1. Set the WLAN country code and IP address.

```
set wlan country-code {code_id}
set interface wireless_interface ip ip_addr/netmask
```

2. Set the SSID.

```
set ssid name name_str
set ssid name_str authentication auth_type encryption encryption_type
set ssid name_str interface interface
(optional) set ssid name_str key-id number
```

3. Set the WLAN mode.

```
set interface wireless_interface wlan both
```

4. Activate wireless changes.

```
save
exec wlan reactivate
```

You can set an SSID to operate in the same subnet as the wired subnet. This action allows clients to work in either interface without having to reconnect in another subnet.

To set an Ethernet and a wireless interface to the same bridge-group interface, use the WebUI or CLI as follows:

### WebUI

Network > Interfaces > List > Edit (*bgroup\_name*) > Bind Port: Select the wireless and ethernet interfaces, then click **Apply**.

### CLI

```
set interface bgroup_name port wireless_interface
set interface bgroup_name port ethernet_interface
```

---

**NOTE:** *Bgroup\_name* can be bgroup0—bgroup3.

*Ethernet\_interface* can be ethernet0/0—ethernet0/4.

*Wireless\_interface* can be wireless0/0—wireless0/3.

If a wireless interface is configured, then you need to reactivate the WLAN with the **exec wlan reactivate** CLI command or click **Activate Changes** on the Wireless > General Settings WebUI page.

---



## Mini PIM Configuration

---

This section explains how to configure the mini physical interface modules (PIMs):

- ADSL2/2 + Interface
- ISDN Interface
- T1 Interface
- E1 Interface
- V.92 Modem Interface

### ADSL2/2+ Interface

Your network uses the ADSL2/2 + interface **adslx/0**, with x representing the mini PIM slot (1 or 2), on the device to connect to the service provider's network through an Asynchronous Transfer Mode (ATM) virtual circuit. You can configure additional virtual circuits by creating ADSL2/2 + subinterfaces. For more information, see "Virtual Circuits" on page 42.

In the WebUI, navigate to the Network > Interfaces > List page to see a list of the current interfaces on the device. If you are using a Telnet or Console session, enter the **get interface** CLI command. You should see that the adslx/0 interface is bound to the Untrust zone.

If you are using the ADSL2/2 + interface to connect to the service network of the provider, you must configure the adsl(x/0) interface. To do this, you must obtain the following information from your service provider:

- Virtual Path Identifier and Virtual Channel Identifier (VPI/VCI) values
- ATM Adaptation Layer 5 (AAL5) multiplexing method, which can be one of the following:
  - Virtual circuit-based multiplexing, in which each protocol is carried over a separate ATM virtual circuit
  - Logical Link Control (LLC) encapsulation, which allows several protocols to be carried on the same ATM virtual circuit (the default multiplexing method)
- Username and password assigned by the service provider for connection to the service provider's network using either Point-to-Point Protocol over Ethernet (PPPoE) or Point-to-Point Protocol over ATM (PPPoA)
- Authentication method, if any, provided for the PPPoE or PPPoA connection
- Optionally, a static IP address and netmask value for your network

## Virtual Circuits

To add virtual circuits, you create subinterfaces to the ADSL2/2+ interface. You can create up to 10 ADSL2/2+ subinterfaces. For example, to create a new subinterface named **adsl1/0.1** bound to the predefined zone named **Untrust**, use the WebUI or CLI as follows:

### WebUI

Network > Interfaces > List > New ADSL Sub-IF: Enter the following, then click **Apply**:

Interface Name: adsl1/0.1  
VPI/VCI: 0/35  
Zone Name: Untrust (select)

### CLI

```
set interface adsl 1/0.1 pvc 0 35 zone Untrust
save
```

You need to configure an ADSL 2/2+ subinterface in the same way as the main ADSL2/2+ interface, including setting the VPI/VCI values, as described in “ADSL2/2+ Interface” on page 41. You configure an ADSL2/2+ subinterface independently of the main ADSL2/2+ interface; that is, you can configure a different multiplexing method, VPI/VCI, and PPP client on the subinterface than on the main ADSL2/2+ interface. You can also configure a static IP address on a subinterface, even if the main ADSL2/2+ interface does not have a static IP address.

## VPI/VCI and Multiplexing Method

Your service provider assigns a VPI/VCI pair for each virtual-circuit connection. For example, you may receive the VPI/VCI pair 1/32, which means a VPI value of 1 and a VCI value of 32. These values must match the values that the service provider has configured on the subscriber’s side of the Digital Subscriber Line Access Multiplexer (DSLAM).

To configure the VPI/VCI pair 1/32 on the adsl1/0 interface, use the WebUI or CLI as follows:

### WebUI

Network > Interfaces > List > Edit (for the adsl1/0 interface): Enter **1/32** in the VPI/VCI field, then click **Apply**.

### CLI

```
set interface adsl1/0 pvc 1 32
save
```

By default, the device uses Logical Link Control (LLC)-based multiplexing for each virtual circuit.

To configure the VPI/VCI 1/32 on the adslx/0 interface and use LLC encapsulation on the virtual circuit, use the WebUI or CLI as follows:

### **WebUI**

Network > Interfaces > List > Edit (for the adsl1/0 interface): Enter the following, then click **Apply**:

VPI/VCI: 1 / 32  
Multiplexing Method: LLC (selected)

### **CLI**

```
set interface adsl1/0 pvc 1 32 mux llc
save
```

## **PPPoE or PPPoA**

An SSG 20 device includes both PPPoE and PPPoA clients to connect to the service provider's network over the ADSL link. PPPoE is the most common form of ADSL encapsulation and is intended for termination on each host on your network. PPPoA is used primarily for business-class service, as PPP sessions can be terminated on the device. To allow the device to connect to the network of the service provider, you need to configure the username and password assigned by the service provider. The configuration for PPPoA is similar to the configuration for PPPoE.

---

**NOTE:** The device supports only one PPPoE session on each virtual circuit.

---

To configure the username **roswell** and password **area51** for PPPoE and bind the PPPoE configuration to the adsl1/0 interface, use the WebUI or CLI as follows:

### **WebUI**

Network > PPP > PPPoE Profile > New: Enter the following, then click **OK**:

PPPoE Instance: poe1  
Bound to Interface: adsl1/0 (select)  
Username: roswell  
Password: area51

### **CLI**

```
set pppoe name poe1 username roswell password area51
set pppoe name poe1 interface adsl1/0
save
```

There are other PPPoE or PPPoA parameters that you can configure on the device, including method of authentication (by default, the device supports either Challenge Handshake Authentication Protocol or Password Authentication Protocol), idle timeout (default is 30 minutes), and so on. Ask your service provider if there are additional PPPoE or PPPoA parameters that you need to configure to enable proper communications with the service provider's server.

## Static IP Address and Netmask

If your service gave you a specific, fixed IP address and netmask for your network, then configure the IP address and netmask for the network and the IP address of the router port connected to the device. You need to also specify that the device is to use the static IP address. (Typically, the device acts as a PPPoE or PPPoA client and receives an IP address for the ADSL interface through negotiations with the PPPoE or PPPoA server.)

You need to configure a PPPoE or PPPoA instance and bind it to the adsl1/0 interface, as described in “PPPoE or PPPoA” on page 43. Make sure that you select **Obtain IP using PPPoE** or **Obtain IP using PPPoA** and the name of the PPPoE or PPPoA instance.

To configure the static IP address 1.1.1.1/24 for the network, use the WebUI or CLI as follows:

### WebUI

Network > Interfaces > List > Edit (for the adsl1/0 interface): Enter the following, then click **Apply**:

IP Address/Netmask: 1.1.1.1/24  
Static IP: (select)

### CLI

```
set interface adsl1/0 ip 1.1.1.1/24
set pppoe name poe1 static-ip
save
```

or

```
set interface adsl1/0 ip 1.1.1.1/24
set pppoa name poa1 static-ip
save
```

To use Domain Name System (DNS) for domain name and address resolution, the computers in your network need to have the IP address of at least one DNS server. If the device receives an IP address for the ADSL2/2+ interface through PPPoE or PPPoA, then it also automatically receives IP addresses for the DNS server(s). If the computers in your network obtain their IP address(es) from the DHCP server on the device, then the computers also obtain these DNS server addresses.

If you assign a static IP address to the ADSL2/2+ interface, then the service provider must give you the IP address(es) of the DNS server(s). You can either configure the DNS server address on each computer in your network or you can configure the DHCP server on the Trust zone interface so that it provides the DNS server address to each computer.

To configure the DHCP server on the bgroup0 interface to provide the DNS server address 1.1.1.152 to computers in your network, use the WebUI or CLI as follows:

### WebUI

Network > DHCP > Edit (for the bgroup0 interface) > DHCP Server: Enter 1.1.1.152 for DNS1, then click **Apply**.

### **CLI**

```
set interface bgroup0 dhcp server option dns1 1.1.1.152
save
```

For more information about configuring the ADSL and ADSL2/2+ interfaces, refer to the *Concepts & Examples ScreenOS Reference Guide*.

## **ISDN Interface**

Integrated Services Digital Network (ISDN) is a set of standards for digital transmission over different media created by the Consultative Committee for International Telegraphy and Telephone (CCITT) and International Telecommunications Union (ITU). As a dial-on-demand service, it has fast call setup and low latency as well as the ability to carry high-quality voice, data, and video transmissions. ISDN is also a circuit-switched service that can be used on both multipoint and point-to-point connections. ISDN provides a service router with a multilink Point-to-Point Protocol (PPP) connection for network interfaces. The ISDN interface is usually configured as the backup interface of the Ethernet interface to access external networks.

To configure the ISDN interface, use the WebUI or CLI as follows:

### **WebUI**

Network > Interfaces > List > Edit (bri1/0): Enter or select the following, then click **OK**:

```
BRI Mode: Dial Using BRI
Primary Number: 123456
WAN Encapsulation: PPP
PPP Profile: isdnprofile
```

### **CLI**

```
set interface bri1/0 dialer-enable
set interface bri1/0 primary-number "123456"
set interface bri1/0 encaps ppp
set interface bri1/0 ppp profile isdnprofile
save
```

To configure the ISDN interface as the backup interface, see “Backup Untrust Interface Configuration” on page 37.

For more information on how to configure the ISDN interface, refer to the *Concepts & Examples ScreenOS Reference Guide*.

## **T1 Interface**

The T1 interface is a basic Physical Layer protocol used by the Digital Signal level 1 (DS-1) multiplexing method in North America. A T1 interface operates at a bit-rate of 1.544 Mbps or speeds up to 24 DS0 channels.

The devices support the following T1 DS-1 standards:

- ANSI T1.107, T1.102
- GR 499-core, GR 253-core

- AT&T Pub 54014
- ITU G.751, G.703

To configure the T1 mini PIM, use the WebUI or CLI as follows:

#### **WebUI**

Network > Interfaces > List > Edit (serial1/0): Enter or select the following, then click **OK**:

WAN Configure: main link  
 WAN Encapsulation: cisco-hdlc  
 Click **Apply**  
 Fixed IP: (select)  
 IP Address/Netmask 172.18.1.1/24

#### **CLI**

```
set interface serial1/0 encap cisco-hdlc
set interface serial1/0 ip 172.18.1.1/24
```

For information on how to configure the T1 interface, refer to the *Concepts & Examples ScreenOS Reference Guide*.

## **E1 Interface**

The E1 interface is a standard wide area network (WAN) digital communications format designed to operate over copper facilities at a rate of 2.048 Mbps. Widely used outside North America, E1 is a basic time-division multiplexing scheme used to carry digital circuits.

The devices support the following E1 standards:

- ITU-T G.703
- ITU-T G.751
- ITU-T G.775

To configure the E1 mini PIM, use the WebUI or CLI as follows:

#### **WebUI**

Network > Interfaces > List > Edit (serial1/0): Enter or select the following, then click **OK**:

WAN Configure: main link  
 WAN Encapsulation: PPP  
 Binding a PPP Profile: junipertest  
 Click **Apply**  
 Fixed IP: (select)  
 IP Address/Netmask 172.18.1.1/24

#### **CLI**

```
set interface serial1/0 encapsulation ppp
set ppp profile "junipertest" static-ip
set ppp profile "junipertest" auth type chap
```

```
set ppp profile "junipertest" auth local-name "juniper"  
set ppp profile "junipertest" auth secret "password"  
set interface serial1/0 ppp profile "junipertest"  
set interface serial1/0 ip 172.18.1.1/24  
set user "server" type wan  
set user "server" password "server"
```

For information on how to configure the E1 interface, refer to the *Concepts & Examples ScreenOS Reference Guide*.

## V.92 Modem Interface

The V.92 interface provides an internal analog modem to establish a PPP connection to a service provider. You can configure the serial interface as a primary or backup interface, which is used in case of interface failover.

---

**NOTE:** The V.92 interface does not work in Transparent mode.

---

To configure the V.92 interface, use the WebUI or CLI as follows:

### WebUI

Network > Interfaces > List > Edit (for serial1/0): Enter the following, then click **OK**:

Zone Name: untrust (select)

ISP: Enter the following, then click **OK**:

ISP Name: isp\_juniper  
Primary Number: 1234567  
Login Name: juniper  
Login Password: juniper

Modem: Enter the following, then click **OK**:

Modem Name: mod1  
Init String: AT&FS7=255S32=6  
Active Modem setting  
Inactivity Timeout: 20

### CLI

```
set interface serial1/0 zone untrust  
set interface serial1/0 modem isp isp_juniper account login juniper password  
juniper  
set interface serial1/0 modem isp isp_juniper primary-number 1234567  
set interface serial1/0 modem idle-time 20  
set interface serial1/0 modem settings mod1 init-strings AT&FS7=255S32=6  
set interface serial1/0 modem settings mod1 active
```

For information on how to configure the V.92 modem interface, refer to the *Concepts & Examples ScreenOS Reference Guide*.

## Basic Firewall Protections

---

The devices are configured with a default policy that permits workstations in the Trust zone of your network to access any resource in the Untrust security zone, while outside computers are not allowed to access or start sessions with your workstations. You can configure policies that direct the device to permit outside computers to start specific kinds of sessions with your computers. For information about creating or modifying policies, refer to the *Concepts & Examples ScreenOS Reference Guide*.

The SSG 20 device provides various detection methods and defense mechanisms to combat probes and attacks aimed at compromising or harming a network or network resource:

- ScreenOS SCREEN options secure a zone by inspecting, and then allowing or denying, all connection attempts that require crossing an interface to that zone. For example, you can apply port-scan protection on the Untrust zone to stop a source from a remote network from trying to identify services to target for further attacks.
- The device applies firewall policies, which can contain content-filtering and Intrusion Detection and Prevention (IDP) components, to the traffic that passes the SCREEN filters from one zone to another. By default, no traffic is permitted to pass through the device from one zone to another. To permit traffic to cross the device from one zone to another, you must create a policy that overrides the default behavior.

To set ScreenOS SCREEN options for a zone, use the WebUI or CLI as follows:

### WebUI

Screening > Screen: Select the zone to which the options apply. Select the SCREEN options that you want, then click **Apply**:

### CLI

```
set zone zone screen option  
save
```

For more information about configuring the network-security options available in ScreenOS, refer to the *Concepts & Examples ScreenOS Reference Guide*.

## Verifying External Connectivity

---

To verify that workstations in your network can access resources on the Internet, start a browser from any workstation in the network and enter the following URL: [www.juniper.net](http://www.juniper.net).



## Resetting a Device to Factory Defaults

---

If you lose the admin password, you can reset the device to its default settings. This action destroys any existing configurations but restores access to the device.



**WARNING:** Resetting the device deletes all existing configuration settings and disables all existing firewall and VPN services.

---

You can restore the device to its default settings in one of the following ways:

- Using a Console connection. For further information, refer to the *Concepts & Examples ScreenOS Reference Guide*.
- Using the reset pinhole on the back panel of the device, as described in the next section.

You can reset the device and restore the factory default settings by pressing the reset pinhole. To perform this operation, you need to either view the device status LEDs on the front panel or start a Console session as described in “Using a Console Connection” on page 28.

To use the reset pinhole to reset and restore the default settings, perform the following steps:

1. Locate the reset pinhole on the rear panel. Using a thin, firm wire (such as a paperclip), push the pinhole for four to six seconds and then release.

The STATUS LED blinks red. A message on the console states that erasure of the configuration has started and the system sends an SNMP/SYSLOG alert.

2. Wait for one to two seconds.

After the first reset, the STATUS LED blinks green; the device is now waiting for the second reset. The Console message now states that the device is waiting for a second confirmation.

3. Push the reset pinhole again for four to six seconds.

The Console message verifies the second reset. The STATUS LED glows red for one-half second and then returns to the blinking green state.

The device then resets to its original factory settings. When the device resets, the STATUS LED glows red for one-half second and then glows green. The console displays device-bootup messages. The system generates SNMP and SYSLOG alerts to configured SYSLOG or SNMP trap hosts.

After the device has rebooted, the console displays the login prompt for the device. The STATUS LED blinks green. The login and password are **netscreen**.

If you do not follow the complete sequence, the reset process cancels without any configuration change and the Console message states that the erasure of the configuration is aborted. The STATUS LED returns to blinking green. If the device did not reset, an SNMP alert is sent to confirm the failure.



## Chapter 4

# Servicing the Device

This chapter describes service and maintenance procedures for an SSG 20 device. It contains the following sections:

- “Required Tools and Parts” on this page
- “Replacing a Mini-Physical Interface Module” on this page
- “Upgrading Memory” on page 54

---

**NOTE:** For safety warnings and instructions, refer to the Juniper Networks *Security Products Safety Guide*. The instructions in the guide warn you about situations that could cause bodily injury. Before working on any equipment, you should be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents.

---

### Required Tools and Parts

---

To replace a component on an SSG 20 device, you need the following tools and parts:

- Electrostatic bag or antistatic mat
- Electrostatic discharge (ESD) grounding wrist strap
- Phillips screwdriver, 1/8-inch

### Replacing a Mini-Physical Interface Module

---

Both SSG 20 models have two slots in the front panel for wide area network mini physical interface modules (WAN mini PIMs). Mini PIMs in an SSG 20 device can be installed and replaced. The device must be powered off before you can remove or install a mini PIM.



**CAUTION:** Make sure the power is off to the device when removing a mini PIM. They are not hot-swappable.

---

## **Removing a Blank Faceplate**

To maintain proper airflow through the SSG 20 device, blank faceplates should remain over slots that do not contain mini PIMs. Do not remove a blank faceplate unless you are installing a mini PIM in its empty slot.

To remove a blank faceplate, perform the following steps:

1. Place an electrostatic bag or antistatic mat on a flat, stable surface on which you intend to place the mini PIM.
2. Attach an ESD grounding strap to your bare wrist and connect the strap to the ESD point on the chassis or to an outside ESD point if the SSG 20 device is disconnected from earth ground.
3. Unplug the power adapter from the device. Verify that the POWER LED is off.
4. Loosen and remove the screws on each side of the faceplate using a screwdriver.
5. Remove the faceplate, then place the faceplate in the electrostatic bag or on the antistatic mat.

## **Removing a Mini PIM**

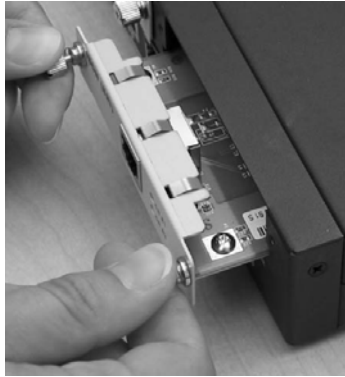
Mini PIMs are installed in the front panel of the SSG 20 device. A mini PIM weighs less than 0.2 lb (106g).

To remove a mini PIM, perform the following steps:

1. Place an electrostatic bag or antistatic mat on a flat, stable surface on which you intend to place the mini PIM.
2. Attach an ESD grounding strap to your bare wrist and connect the strap to the ESD point on the chassis or to an outside ESD point if the SSG 20 device is disconnected from earth ground.
3. Unplug the power adapter from the device. Verify that the POWER LED is off.
4. Label the cables connected to the mini PIM so that you can later reconnect each cable to the correct mini PIM.
5. Disconnect the cables from the mini PIM.
6. If necessary, arrange the cables to prevent them from dislodging or developing stress points:
  - a. Secure the cables so that they are not supporting their own weight as they hang to the floor.
  - b. Place any excess cables out of the way in neatly coiled loops.
  - c. Use fasteners to maintain the shape of the cable loops.
7. Loosen and remove the screws on each side of the mini PIM faceplate using a screwdriver.

8. Grasp the screws on each side of the mini PIM faceplate and slide the mini PIM out of the device. Place the mini PIM in the electrostatic bag or on the antistatic mat.

**Figure 16: Removing a Mini PIM**



9. If you are not reinstalling a mini PIM into the empty slot, install a blank faceplate over the slot to maintain proper airflow.

### ***Installing a Mini PIM***

To install a mini PIM, perform the following steps:

1. Attach an ESD grounding strap to your bare wrist and connect the strap to the ESD point on the chassis or to an outside ESD point if the SSG 20 device is disconnected from earth ground.
2. Unplug the power adapter from the device. Verify that the POWER LED is off.
3. Grasp the screws on each side of the mini PIM faceplate and align the notches in the connector at the rear of the mini PIM with the notches in the mini PIM slot in the SSG 20 device. Then slide the mini PIM in until it lodges firmly in the device.

**Figure 17: Installing a Mini PIM**



**CAUTION:** Slide the mini PIM straight into the slot to avoid damaging the components on the mini PIM.

---

4. Tighten the screws on each side of the mini PIM faceplate using a 1/8-inch slotted screwdriver.
5. Insert the appropriate cables into the cable connectors on the mini PIM.

6. If necessary, arrange the cables to prevent them from dislodging or developing stress points:
  - a. Secure the cables so that they are not supporting their own weight as they hang to the floor.
  - b. Place any excess cables out of the way in neatly coiled loops.
  - c. Use fasteners to maintain the shape of the cable loops.
7. Unplug the power adapter from the device. Verify that the POWER LED glows steadily green after you press the power button.
8. Verify that the PIM status LED on the system dashboard glows steadily green to confirm that the mini PIM is online.

## Upgrading Memory

---

You can upgrade an SSG 20 device from a single 128 MB dual in-line memory module (DIMM) dynamic random access memory (DRAM) to a 256 MB DIMM DRAM.

To upgrade the memory on an SSG 20 device, perform the following steps:

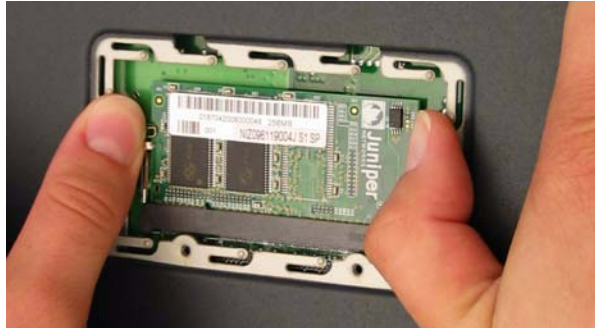
1. Attach an ESD grounding strap to your bare wrist and connect the strap to the ESD point on the chassis or to an outside ESD point if the device is disconnected from earth ground.
2. Unplug the AC cord from the power outlet.
3. Turn over the device so that its top is lying on a flat surface.
4. Use a phillips screwdriver to remove the screws from the memory-card cover. Keep the screws nearby for use when securing the cover later.
5. Remove the memory-card cover.

**Figure 18: Bottom of Device**



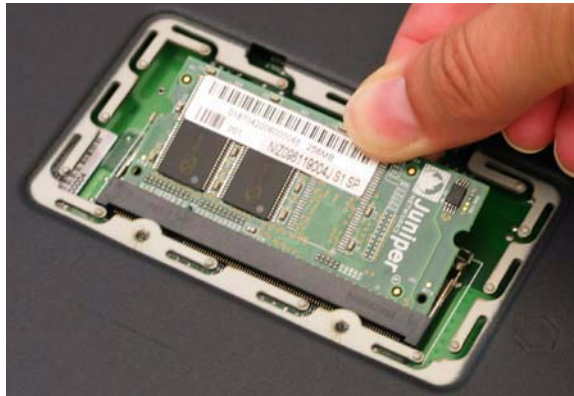
6. Release the 128 MB DIMM DRAM by pressing your thumbs outward on the locking tabs on each side of the module so that the tabs move away from the module.

**Figure 19: Unlocking the Memory Module**



7. Grip the long edge of the memory module and slide it out. Set it aside.

**Figure 20: Removing Module Slots**



8. Insert the 256 MB DIMM DRAM into the slot. Exerting even pressure with both thumbs upon the upper edge of the module, press the module downward until the locking tabs click into position.

**Figure 21: Inserting the Memory Module**



9. Place the memory-card cover over the slot.
10. Use the phillips screwdriver to tighten the screws, securing the cover to the device.



## Appendix A

# Specifications

This appendix provides general system specifications for an SSG 20 device. It contains the following sections:

- “Physical” on page 58
- “Electrical” on page 58
- “Environmental Tolerance” on page 58
- “Certifications” on page 59
- “Connectors” on page 60

## Physical

**Table 8: SSG 20 Physical Specifications**

Description	Value
Chassis dimensions	294 mm x 194.8 mm x 44 mm (11.5 inches x 7.7 inches x 2 inches)
Device weight	1.53 kg (3.3 lbs) without PIMs installed
ISDN PIM	70g
ADSL Annex A PIM	106g
ADSL Annex B PIM	106g
T1 PIM	75g
E1 PIM	75g
V.92 PIM	79g

## Electrical

**Table 9: SSG 20 Electrical Specifications**

Item	Specification
DC input voltage	12V
DC system current rating	3 - 4.16 Amps

## Environmental Tolerance

**Table 10: SSG 20 Environmental Tolerance**

Description	Value
Altitude	No performance degradation to 6,600 ft (2,000 m)
Relative humidity	Normal operation ensured in relative humidity range of 10 to 90 percent, noncondensing
Temperature	Normal operation ensured in temperature range of 32°F (0°C) to 104°F (40°C) Nonoperating storage temperature in shipping carton: -4°F (-20°C) to 158°F (70°C)

## **Certifications**

---

### **Safety**

- CAN/CSA-C22.2 No. 60950-1-03/UL 60950-1 Safety of Information Technology Equipment
- EN 60950-1 (2000) Third Edition Safety of Information Technology Equipment
- IEC 60950-1 (1999) Third Edition Safety of Information Technology Equipment

### **EMC Emissions**

- FCC Part 15 Class B (USA)
- EN 55022 Class B (Europe)
- AS 3548 Class B (Australia)
- VCCI Class B (Japan)

### **EMC Immunity**

- EN 55024
- EN-61000-3-2 Power Line Harmonics
- EN-61000-3-3 Power Line Harmonics
- EN-61000-4-2 ESD
- EN-61000-4-3 Radiated Immunity
- EN-61000-4-4 EFT
- EN-61000-4-5 Surge
- EN-61000-4-6 Low Frequency Common Immunity
- EN-61000-4-11 Voltage Dips and Sags

### **ETSI**

European Telecommunications Standards Institute (ETSI) EN-300386-2: Telecommunication Network Equipment. Electromagnetic Compatibility Requirements; (equipment category–Other than telecommunication centers)

## T1 Interface

- FCC Part 68 - TIA 968
- Industry Canada CS-03
- UL 60950-1 Applicable requirements for TNV circuit with outside plant lead connection

## Connectors

Figure 22 shows the location of the pins on the RJ-45 connector.

**Figure 22: RJ-45 Pinouts**

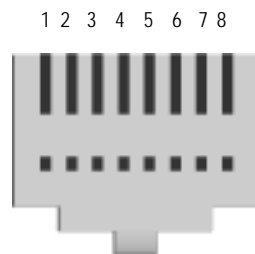


Table 11 lists the RJ-45 connector pinouts.

**Table 11: RJ-45 Connector Pinouts**

Pin	Name	I/O	Description
1	RTS Out	O	Request To Send
2	DTR Out	O	Data Terminal Ready
3	TxD	O	Transmit Data
4	GND	N/A	Chassis Ground
5	GND	N/A	Chassis Ground
6	RxD	I	Receive Data
7	DSR	I	Data Set Ready
8	CTS	I	Clear To Send

Figure 23 shows the location of the pins on the DB-9 female connector.

**Figure 23: DB-9 Female Connector**

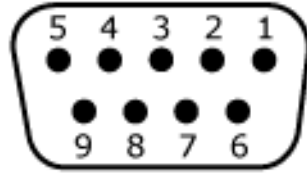


Table 12 provides the DB-9 connector pinouts.

**Table 12: DB-9 Connector Pinouts**

Pin	Name	I/O	Description
1	DCD	I	Carrier Detect
2	RxD	I	Receive Data
3	TxD	O	Transmit Data
4	DTR	O	Data Terminal Ready
5	GND	N/A	Signal Ground
6	DSR	I	Data Set Ready
7	RTS	O	Request To Send
8	CTS	I	Clear To Send
9	RING	I	Ring Indicator



## Appendix B

# Initial Configuration Wizard

This appendix provides detailed information about the Initial Configuration Wizard (ICW) for an SSG 20 device.

After you have physically connected your device to the network, you can use the ICW to configure the interfaces that are installed on your device.

This section describes the following ICW windows:

- Rapid Deployment Window on page 64
- Administrator Login Window on page 64
- WLAN Access Point Window on page 65
- Physical Interface Window on page 65
- ADSL2/2+ Interface Window on page 66
- T1 Interface Windows on page 68
- E1 Interface Windows on page 73
- ISDN Interface Windows on page 75
- V.92 Modem Interface Window on page 78
- Eth0/0 Interface (Untrust Zone) Window on page 78
- Eth0/1 Interface (DMZ Zone) Window on page 79
- Bgroup0 Interface (Trust Zone) Window on page 80
- Wireless0/0 Interface (Trust Zone) Window on page 81
- Interface Summary Window on page 82
- Physical Ethernet DHCP Interface Window on page 83
- Wireless DHCP Interface Window on page 83
- Confirmation Window on page 84

## 1. Rapid Deployment Window

**Figure 24: Rapid Deployment Window**

If your network uses NetScreen-Security Manager (NSM), you can use a Rapid Deployment configlet to automatically configure the device. Obtain a configlet from your NSM administrator, select **Yes**, select **Load Configlet from:**, browse to the file location, then click **Next**. The configlet sets up the device for you, so you don't need to use the following steps to configure the device.

If you want to bypass the ICW and go directly to the WebUI, select the last option, then click **Next**.

If you are not using a configlet to configure the device and want to use the ICW, select the first option, then click **Next**. The ICW Welcome screen appears. Click **Next**. The Administrator Login window appears.

## 2. Administrator Login Window

Enter a new administrator login name and password, then click **Next**.

**Figure 25: Administrator Login Window**



### 3. WLAN Access Point Window

If you are using the device in the WORLD or ETSI regulatory domain, you must choose a country code. Select the appropriate options, then click **Next**.

**Figure 26: Wireless Access Point Country Code Window**

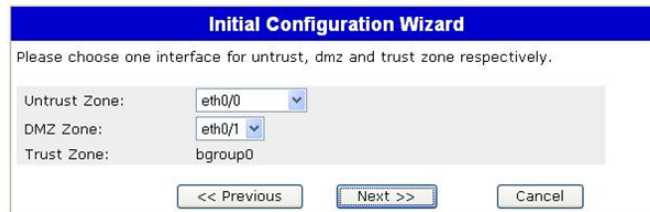


The screenshot shows the 'Initial Configuration Wizard' window. The title bar is blue with the text 'Initial Configuration Wizard'. Below the title bar, the text reads 'How do you want to configure the wireless access point?'. There are four dropdown menus: 'Regulatory Domain' is set to 'WORLD', 'Country Code' is set to 'NO\_COUNTRY\_SET', '2.4G Mode' is set to '802.11b/g', and '5G Mode' is set to '802.11a'. Below these is a checkbox labeled 'Configure wireless0/0 interface in trust zone.' which is checked. At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

### 4. Physical Interface Window

On the interface-to-zone bindings screen, you set the interface to which you want to bind the Untrust security zone. Bgroup0 is prebound to the Trust security zone. Eth0/1 is bound to the DMZ security zone but is optional.

**Figure 27: Physical Interface Window**



The screenshot shows the 'Initial Configuration Wizard' window. The title bar is blue with the text 'Initial Configuration Wizard'. Below the title bar, the text reads 'Please choose one interface for untrust, dmz and trust zone respectively.'. There are three dropdown menus: 'Untrust Zone' is set to 'eth0/0', 'DMZ Zone' is set to 'eth0/1', and 'Trust Zone' is set to 'bgroup0'. At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

After binding an interface to a zone, you can configure the interface. The configuration windows that are displayed after this point depend on which mini-PIMs are installed in your security device. To continue configuring your device with the ICW, click **Next**.

### 5. ADSL2/2+ Interface Window

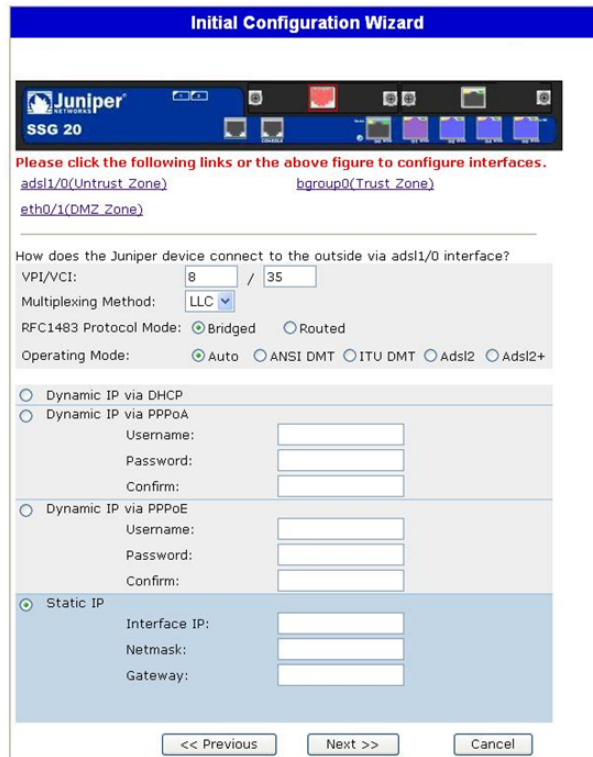
If you have the ADSL2/2 + mini P1M installed in your device, you can configure the adslx/0 interface using the following window.

---

**NOTE:** If you have two ADSL2/2 + mini-P1Ms installed on your device, you cannot configure the Multi-link feature with the ICW. To configure ML ADSL, refer to the *Concepts & Examples ScreenOS Reference Guide*.

---

**Figure 28: ADSL Interface Configuration Window**



**Table 13: Fields in ADSL Interface Configuration Window**

Field	Description
<b>Information from Service Provider:</b>	
VPI/VCI	VPI/VCI values to identify the permanent virtual circuit.
Multiplexing Method	ATM multiplexing method ( <b>LLC</b> is the default).
RFC1483 Protocol Mode	Protocol mode setting ( <b>Bridged</b> is the default).
Operating Mode	Operating mode for the physical line ( <b>Auto</b> is the default).
IP configuration settings	<ul style="list-style-type: none"><li>■ Select <b>Dynamic IP via DHCP</b> to enable the device to receive an IP address for the ADSL interface from a service provider.</li><li>■ Select <b>Dynamic IP via PPPoA</b> to enable the device to act as a PPPoA client. Enter the username and password assigned by the service provider.</li><li>■ Select <b>Dynamic IP via PPPoE</b> to enable the device to act as a PPPoE client. Enter the username and password assigned by the service provider.</li><li>■ Select <b>Static IP</b> to assign a unique and fixed IP address to the ADSL interface. Enter the interface IP address, netmask, and gateway (the gateway address is the IP address of the router port connected to the device).</li></ul>

If you do not know these settings, refer to the *Common Settings for Service Providers* document that came with the service provider device.

## 6. T1 Interface Windows

If you have the T1 mini-PIM installed in your device and you selected the Frame Relay option, the following windows are displayed:

- T1 Physical Layer Tab Window
- T1 Frame Relay Tab Window

---

**NOTE:** If you have two T1 mini-PIMs installed on your device and you select the Multi-link option, you will see two Physical Layer tabs.

---

**Figure 29: T1 Physical Layer Tab Window**

The screenshot shows the 'Initial Configuration Wizard' for a Juniper SSG 20. The window title is 'Initial Configuration Wizard'. Below the title bar, there is a navigation bar with the Juniper logo and 'SSG 20'. The main content area contains the following text:

Please click the following links or the above figure to configure interfaces.  
[serial1/0\(Untrust\\_Zone\)](#)      [bgroup0\(Trust\\_Zone\)](#)  
[eth0/1\(DMZ\\_Zone\)](#)

How does the Juniper device connect to the outside via serial1/0(T1) interface?  
 WAN Encapsulation:  Frame Relay    PPP    Cisco HDLC

The 'Physical Layer' tab is selected. The configuration options are as follows:

Clocking:	<input checked="" type="radio"/> External	<input type="radio"/> Internal (Lab Use Only)
Line Buildout:	0~132 Feet	
Line Encoding:	<input type="radio"/> AMI (Auto Mark Inversion)	<input checked="" type="radio"/> B8ZS (8-bits Zero Suppression)
Byte Encoding:	<input type="radio"/> 7-bits per byte	<input checked="" type="radio"/> 8-bits per byte
Frame Checksum:	<input checked="" type="radio"/> 16-bits	<input type="radio"/> 32-bits
Framing Mode:	<input type="radio"/> Super Frame	<input checked="" type="radio"/> Extended Super Frame
Idle Cycles Flag:	<input checked="" type="radio"/> 0x7E	<input type="radio"/> 0xFF(All Ones)
Start/End Flags:	<input checked="" type="radio"/> Filler	<input type="radio"/> Share
Invert data:	<input type="checkbox"/>	
Loopback Respond:	<input type="checkbox"/>	
Time Slots:	0	(0(all active), 1..24(e.g. 2,7-9))

At the bottom of the window, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

**Table 14: Fields in T1 Physical Layer Tab Window**

<b>Field</b>	<b>Description</b>
Clocking	Sets the transmit clock on the interface.
Line Buildout	Sets the distance at which an interface drives a line. Default setting is 0 - 132 feet.
Line Encoding	Sets the line encoding format on the interface: <ul style="list-style-type: none"><li>■ Auto Mark Inversion</li><li>■ 8-bits zero suppression</li></ul>
Byte Encoding	Sets the byte encoding on the T1 interface to use 7 bits per byte or 8 bits per byte. Default is 8 bits per byte.
Frame Checksum	Sets the size of checksum. Default is <b>16</b> .
Framing Mode	Sets the framing format. Default is <b>Extended mode</b> .
Idle Cycles Flag	Sets the value that the interface transmits during idle cycles. Default setting is <b>0x7E</b> : <ul style="list-style-type: none"><li>■ 0x7E (flags)</li><li>■ 0xFF (ones)</li></ul>
Start/End Flags	Sets the transmission of start and end flags to either filler or shared. The default is <b>filler</b> .
Invert Data checkbox	Enables inverted transmission of unused data bits.
Loopback Respond checkbox	Enables loopback on the T1 interface from the remote channel service unit (CSU).
Time Slots	Sets the use of time slots on a T1 interface. Default is <b>0</b> , all 24 time slots used.

**Figure 30: T1 Frame Relay Tab Window**



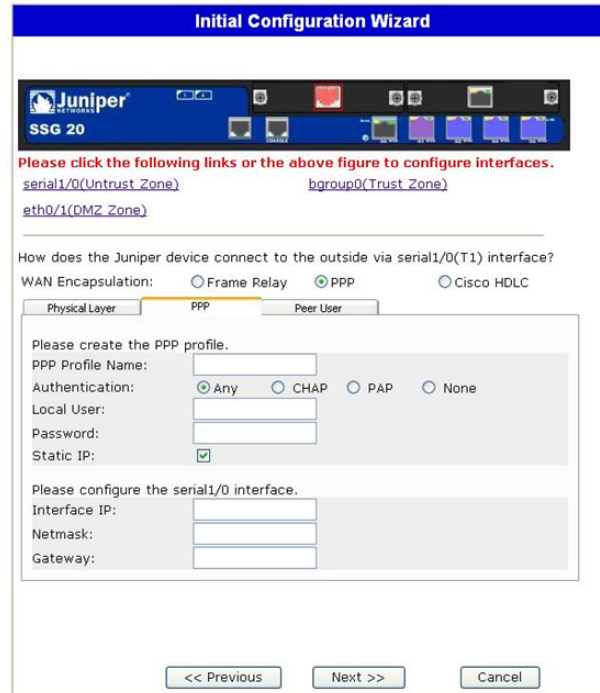
**Table 15: Fields in T1 Frame Relay Tab Window**

Field	Description
No-Keepalive checkbox	Enables no-keepalives.
Type	Sets the frame relay LMI type: <ul style="list-style-type: none"> <li>■ ANSI: American National Standards Institute supports data rates up to 8Mbps downstream and 1Mbps upstream.</li> <li>■ ITU: International Telecommunications Union supports data rates of 6.144 Mbps downstream and 640 kbps upstream.</li> </ul>
Interface Name	Sets the subinterface name.
Inverse ARP	Enables inverse Address Resolution Protocol for the subinterface.
Frame Relay DLCI	Assigns a data link connection identifier (DLCI) to the subinterface.
Interface IP	Sets the IP address for the subinterface.
Netmask	Sets the netmask for the subinterface.
Gateway	Sets the gateway address for the subinterface.

If you have the T1 mini-PIM installed in your device and you selected the PPP option, the following additional windows are displayed:

- PPP Option with PPP Tab Window
- PPP Option with Peer User Tab Window

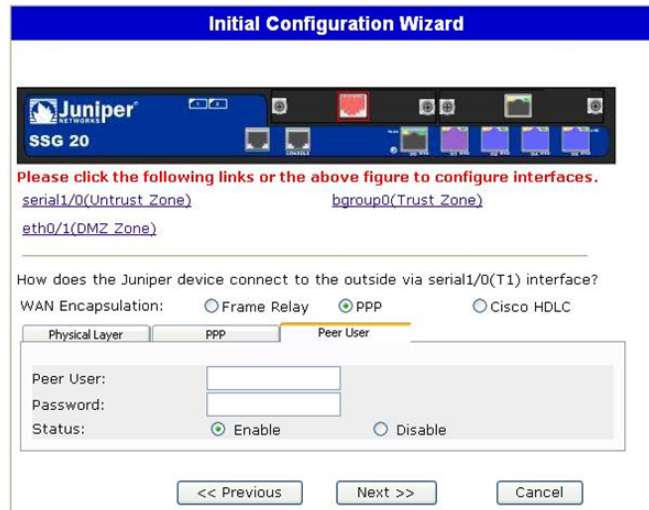
**Figure 31: PPP Option with PPP Tab Window**



**Table 16: Fields in PPP Option with PPP Tab Window**

Field	Description
PPP Profile Name	Sets the name of the PPP profile
Authentication	Sets the authentication type
Local User	Sets the name of the local user
Password	Sets the password for the local user
Static IP checkbox	Enables a static IP address
Interface IP	Sets the serialx/0 interface IP address
Netmask	Sets the serialx/0 netmask
Gateway	Sets the serialx/0 gateway address

**Figure 32: PPP Option with Peer User Tab Window**

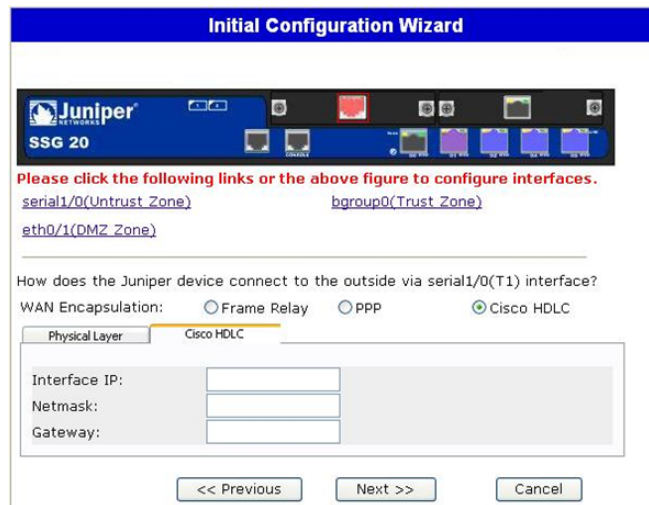


**Table 17: Fields in PPP Option with Peer User Tab Window**

Field	Description
Peer User	Sets the name of the peer user
Password	Sets the password for the peer user specified in the Peer User text field
Status	Enables or disables PPP

If you have the T1 mini-PIM installed in your device and you selected the Cisco HDLC option, the following window is displayed:

**Figure 33: Cisco HDLC Option with Cisco HDLC Tab Window**





**Table 18: Fields in Cisco HDLC Option with Cisco HDLC Tab Window**

Field	Description
Interface IP	Sets the IP address for the T1 Cisco HDLC interface
Netmask	Sets the netmask for the T1 Cisco HDLC interface
Gateway	Sets the gateway address for the T1 Cisco HDLC interface

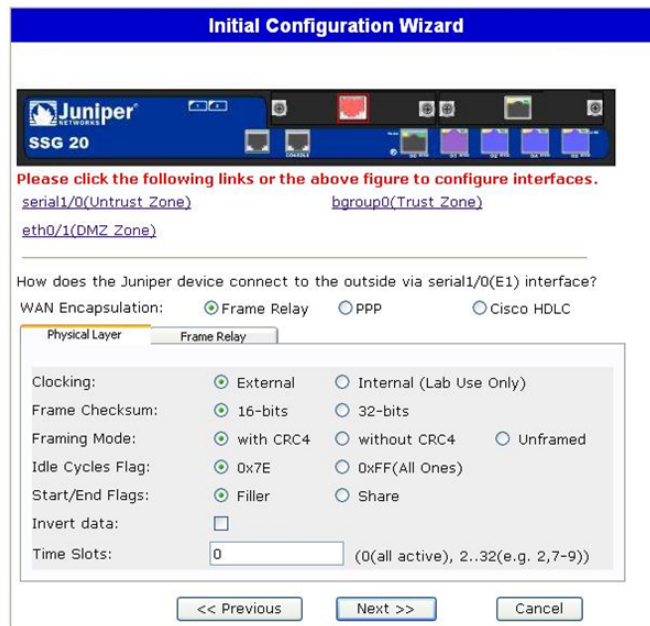
## 7. E1 Interface Windows

If you have the E1 mini-PIM installed in your device and you selected the Frame Relay option, the following windows are displayed:

- E1 Physical Layer Tab Window
- E1 Frame Relay Tab Window

**NOTE:** If you have two E1 mini PIMs installed on your device and you select the Multi-link option, you will see two Physical Layer tabs.

**Figure 34: E1 Physical Layer Tab Window**



**Table 19: Fields in E1 Physical Layer Tab Window**

Field	Description
Clocking	Sets the transmit clock on the interface.
Frame Checksum	Sets the size of checksum. Default is <b>16</b> .
Framing Mode	Sets the framing format. Default is <b>without CRC4</b> .
Idle Cycles Flag	Sets the value that the interface transmits during idle cycles. Default setting is <b>0x7E</b> : <ul style="list-style-type: none"> <li>■ 0x7E (flags)</li> <li>■ 0xFF (ones)</li> </ul>
Start/End Flags	Sets the transmission of start and end flags to either filler or shared. The default is filler.
Invert Data checkbox	Enables inverted transmission of unused data bits.
Time Slots	Sets the use of time slots on a T1 interface. Default is <b>0</b> , all 32 time slots used.

**Figure 35: E1 Frame Relay Tab Window**



**Table 20: Fields in E1 Frame Relay Tab Window**

Field	Description
No-Keepalive checkbox	Enables no-keepalives.
Type	Sets the frame relay LMI type: <ul style="list-style-type: none"> <li>■ ANSI: American National Standards Institute supports data rates up to 8Mbps downstream and 1Mbps upstream.</li> <li>■ ITU: International Telecommunications Union supports data rates of 6.144 Mbps downstream and 640 kbps upstream.</li> </ul>
Interface Name	Sets the subinterface name.
Inverse ARP checkbox	Enables inverse Address Resolution Protocol (ARP) for the subinterface.
Frame Relay DLCI	Assigns a DLCI to the subinterface.

Field	Description
Interface IP	Sets the IP address for the subinterface
Netmask	Sets the netmask for the subinterface
Gateway	Sets the gateway address for the subinterface

To configure the E1 interface with PPP options, see “PPP Option with PPP Tab Window” on page 71.

To configure the E1 interface with the Cisco HDLC, see “Cisco HDLC Option with Cisco HDLC Tab Window” on page 72.

## 8. ISDN Interface Windows

If you have the ISDN mini-PIM installed in your device, you can configure the brix/0 (Untrust) interface using the following window.

**NOTE:** If you have two ISDN mini PIMs installed in your device and you selected the Multi-link option, you will see two Physical Layer tabs.

**Figure 36: ISDN Physical Layer Tab Window**

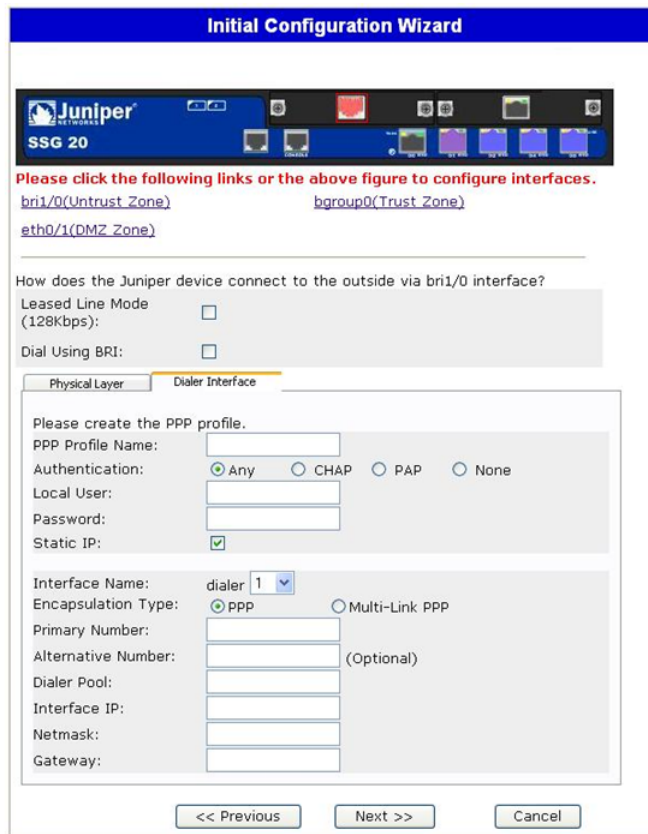


**Table 21: Fields in ISDN Physical Layer Tab Window**

Field	Description
Switch Type	Sets the service provider switch type: <ul style="list-style-type: none"> <li>■ att5e: At&amp;T 5ESS</li> <li>■ ntdms100: Nortel DMS 100</li> <li>■ ins-net: NTT INS-Net</li> <li>■ etsi: European variants</li> <li>■ ni1: National ISDN-1</li> </ul>
SPID1	Service Provider ID, usually a seven-digit telephone number with some optional numbers. Only the DMS-100 and NI1 switch types require SPIDs. The DMS-100 switch type has two SPIDs assigned, one for each B-channel.
SPID2	Backup service provider ID.
TEI Negotiation	Specifies when to negotiate TEI, either at startup or on the first call. Typically this setting is used for ISDN service offerings in Europe and connections to DMS-100 switches that are designed to initiate TEI negotiation.
Calling Number	ISDN network billing number.
Sending Complete checkbox	Enables sending of complete information to outgoing setup message. Usually only used in Hong Kong and Taiwan.

You can select the bri1/0 interface to connect using dialer, multi-link dialer, leased line, or dial with BRI. Selecting neither, one, or both options displays a window similar to the following.

**Figure 37: ISDN Connection Tab Window**



**Table 22: Fields in ISDN Connection Tab Window**

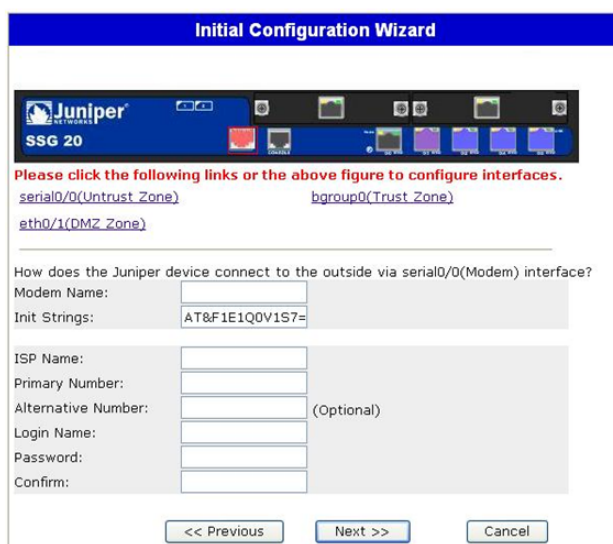
Field	Description
PPP Profile Name	Sets a PPP profile name to the ISDN interface.
Authentication	Sets the PPP authentication type: <ul style="list-style-type: none"> <li>■ Any</li> <li>■ CHAP: Challenge Handshake Authentication Protocol</li> <li>■ PAP: Password Authentication Protocol</li> <li>■ None</li> </ul>
Local User	Sets the local user.
Password	Sets the password for the local user.
Static IP checkbox	Enables a static IP address for the interface.
Interface IP	Sets the interface IP address.
Interface Name (Dialer only)	Sets the dialer interface name. Default is <b>dialer.1</b> .
Encapsulation Type	Sets the encapsulation type on the dialer and dialer using BRI interface. Default is <b>PPP</b> .
Primary Number	Sets the primary number for dialer and dialer using BRI interfaces.
Alternative Number	Sets the alternative (secondary) number to be used when the primary number cannot be used for connectivity.

Field	Description
Dialer Pool (Dialer only)	Sets the dialer pool name for the dialer interface.
Netmask	Sets the netmask.
Gateway	Sets the gateway address.

### 9. V.92 Modem Interface Window

If you have the V.92 mini-PIM installed in your device, you can configure the serialx/0 (Modem) interface using the following window:

**Figure 38: Modem Interface Window**



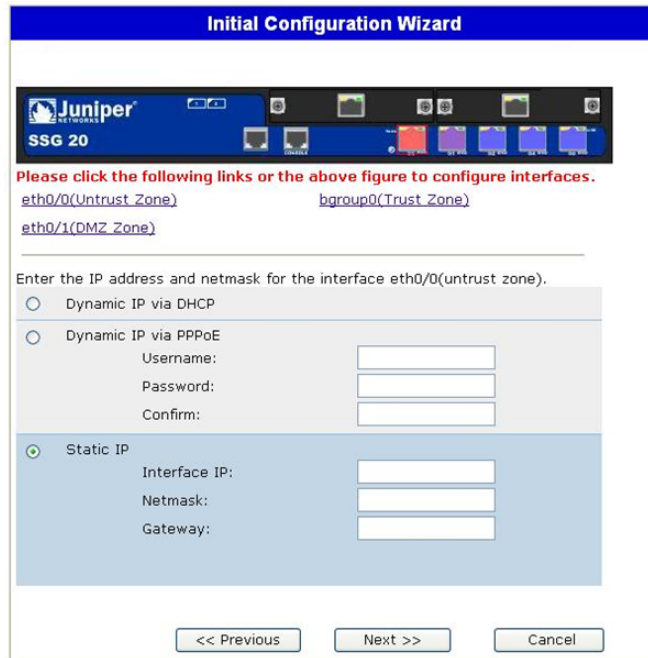
**Table 23: Fields in Modem Interface Window**

Field	Description
Modem Name	Sets the name for the modem interface
Init String	Sets the initialization string for the modem
ISP Name	Assigns a name to the service provider
Primary Number	Specifies the phone number to access the service provider
Alternative Number (optional)	Specifies an alternative phone number to access the service provider if the primary number does not connect
Login Name	Sets the login name for the service provider account
Password	Sets the password for the login name
Confirm	Confirms the password typed in the Password field

### 10. Eth0/0 Interface (Untrust Zone) Window

The eth0/0 interface can have a static or a dynamic IP address assigned via DHCP or PPPoE.

**Figure 39: Eth0/0 Interface Window**



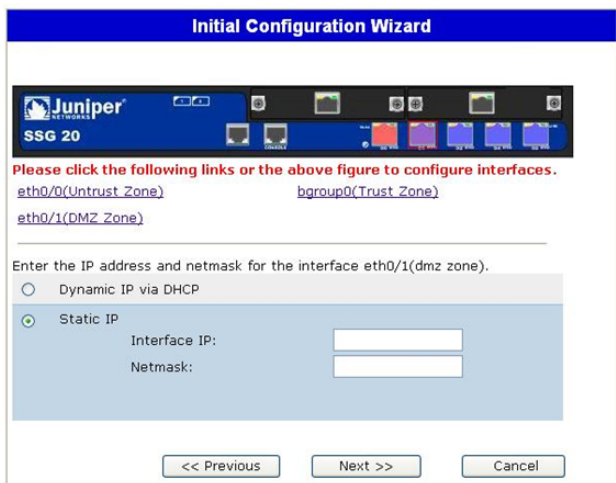
**Table 24: Fields in Eth0/0 Interface Window**

Field	Description
Dynamic IP via DHCP	Enables the device to receive an IP address for the Untrust zone interface from a service provider.
Dynamic IP via PPPoE	Enables the device to act as a PPPoE client, receiving an IP address for the Untrust zone interface from a service provider. Enter the username and password assigned by the service provider.
Static IP	Assigns a unique and fixed IP address to the Untrust zone interface. Enter the Untrust zone interface IP address, netmask, and gateway address.

## 11. Eth0/1 Interface (DMZ Zone) Window

The eth0/1 interface can have a static or a dynamic IP address assigned via DHCP.

**Figure 40: Eth0/1 Interface Window**



**Table 25: Fields in Eth0/1 Interface Window**

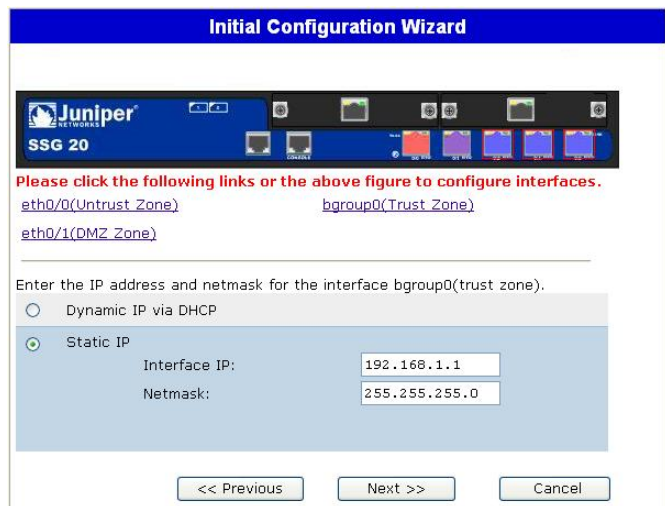
Field	Description
Dynamic IP via DHCP	Enables the device to receive an IP address for the DMZ interface from a service provider.
Static IP	Assigns a unique and fixed IP address to the DMZ interface. Enter the DMZ interface IP and netmask.

## 12. Bgroup0 Interface (Trust Zone) Window

The bgroup0 interface can have a static or a dynamic IP address assigned via DHCP.

The default interface IP address is **192.168.1.1** with a netmask of **255.255.255.0** or **24**.

**Figure 41: Bgroup0 Interface Window**





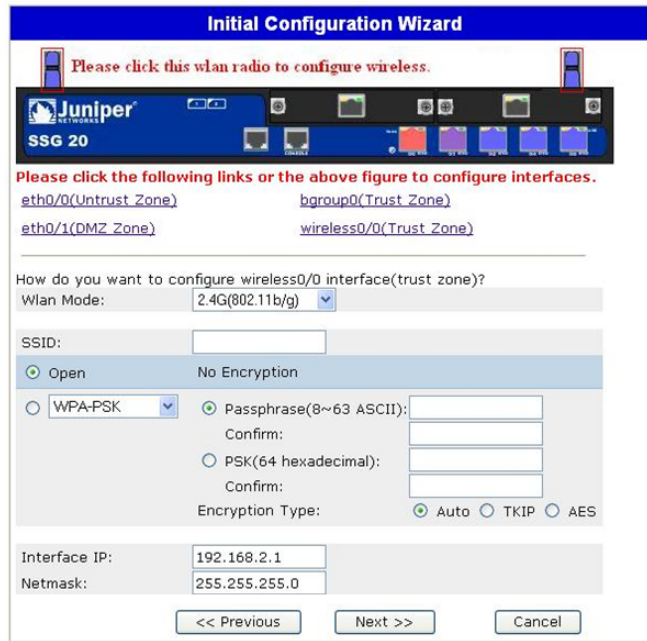
**Table 26: Fields in Bgroup0 Interface Window**

Field	Description
Dynamic IP via DHCP	Enables the device to receive an IP address for the Trust zone interface from a service provider.
Static IP	Assigns a unique and fixed IP address to the Trust zone interface. Enter the Trust zone interface IP address and netmask.

### 13. Wireless0/0 Interface (Trust Zone) Window

If you are configuring the SSG 20-WLAN device, you must set a Service Set Identifier (SSID) before the wireless0/0 interface can be activated. For detailed instructions about configuring your wireless interface(s), refer to the *Concepts & Examples ScreenOS Reference Guide*.

**Figure 42: Wireless0/0 Interface Window**



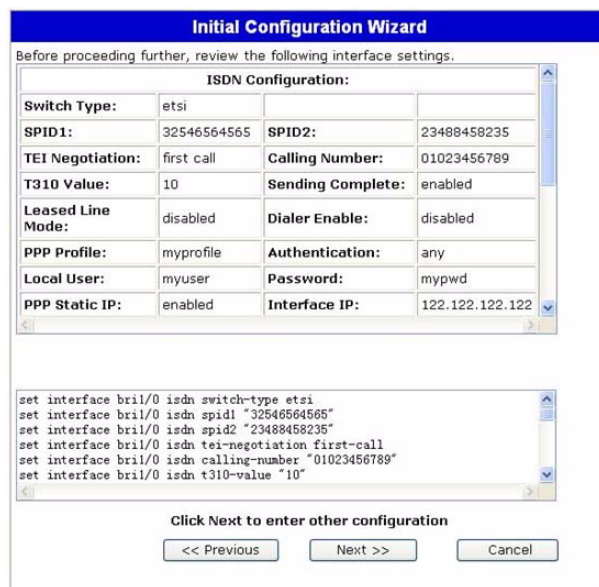
**Table 27: Fields in Wireless0/0 Interface Window**

Field	Description
Wlan Mode	Sets the WLAN radio mode: <ul style="list-style-type: none"> <li>■ 5G (802.11 a).</li> <li>■ 2.4G (802.11b/g).</li> <li>■ Both (802.11 a/b/g).</li> </ul>
SSID	Sets the SSID name.
Authentication and Encryption	Sets the WLAN interface authentication and encryption: <ul style="list-style-type: none"> <li>■ <b>Open</b> authentication, the default, allows anyone to access the device. There is no encryption for this authentication option.</li> <li>■ <b>WPA Pre-Shared Key</b> authentication sets the Pre-Shared Key (PSK) or passphrase that must be entered when accessing a wireless connection. You can choose to enter a HEX or an ASCII value for the PSK. A HEX PSK must be a 256-bit (64-text character) HEX value. An ASCII passphrase must be 8 to 63 text characters. You must select Temporal Key Integrity Protocol (<b>TKIP</b>) or Advanced Encryption Standard (<b>AES</b>) as the encryption type for this option, or select <b>Auto</b> to allow either option.</li> <li>■ WPA2 Pre-Shared Key.</li> <li>■ WPA Auto Pre-Shared Key.</li> </ul>
Interface IP	Sets the WLAN interface IP address.
Netmask	Sets the WLAN interface netmask.

### 14. Interface Summary Window

After you have configured the WAN interfaces, you will see the Interface Summary window.

**Figure 43: Interface Summary Window**



Check your interface configuration, then click **Next** when ready to proceed. The Physical Ethernet DHCP Interface window appears.

### 15. Physical Ethernet DHCP Interface Window

Select **Yes** to enable your device to assign IP addresses to your wired network via DHCP. Enter the IP address range that you want your device to assign to clients using your network, then click **Next**.

**Figure 44: Physical Ethernet DHCP Interface Window**

The screenshot shows the 'Initial Configuration Wizard' window. The title bar is blue with the text 'Initial Configuration Wizard'. Below the title bar, there is a question: 'Do you want the Juniper device to dynamically assign IP addresses to your local **wired** hosts using DHCP? If so, select Yes and enter an IP address range from which to assign the addresses.' There are two radio buttons: 'Yes' and 'No'. The 'No' radio button is selected. Below the radio buttons, there are four input fields: 'IP Address Range Start' (192.168.1.33), 'End' (192.168.1.126), 'DNS Server 1 (optional)', and 'DNS Server 2 (optional)'. At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

### 16. Wireless DHCP Interface Window

Select **Yes** to enable your device to assign IP addresses to your wireless network via DHCP. Enter the IP address range that you want your device to assign to clients using your network, then click **Next**.

**Figure 45: Wireless DHCP Interface Window**

The screenshot shows the 'Initial Configuration Wizard' window. The title bar is blue with the text 'Initial Configuration Wizard'. Below the title bar, there is a question: 'Do you want the Juniper device to dynamically assign IP addresses to your local **wireless** hosts using DHCP? If so, select Yes and enter an IP address range from which to assign the addresses.' There are two radio buttons: 'Yes' and 'No'. The 'No' radio button is selected. Below the radio buttons, there are four input fields: 'IP Address Range Start' (192.168.2.33), 'End' (192.168.2.126), 'DNS Server 1 (optional)', and 'DNS Server 2 (optional)'. At the bottom, there are three buttons: '<< Previous', 'Next >>', and 'Cancel'.

## 17. Confirmation Window

Confirm your device configuration and change as needed. Click **Next** to save, reboot the device, and run the configuration.

**Figure 46: Confirmation Window**

**Initial Configuration Wizard**

Before proceeding further, review the following all device settings.

<b>Admin Login:</b>	netscreen	<b>Password:</b>	*****
<b>Device is in NAT mode.</b>			
<b>ISDN Configuration:</b>			
<b>Switch Type:</b>	etsi		
<b>SPID1:</b>	32546564565	<b>SPID2:</b>	23488458235
<b>TEI Negotiation:</b>	first call	<b>Calling Number:</b>	01023456789
<b>T310 Value:</b>	10	<b>Sending Complete:</b>	enabled
<b>Leased Line Mode:</b>	disabled	<b>Dialer Enable:</b>	disabled
<b>PPP Profile:</b>	myprofile	<b>Authentication:</b>	any

```
set admin password "netscreen"
set interface br1/0 isdn switch-type etsi
set interface br1/0 isdn spid1 "32546564565"
set interface br1/0 isdn spid2 "23488458235"
set interface br1/0 isdn tei-negotiation first-call
set interface br1/0 isdn calling-number "01023456789"
```

Click Next to save CLI into device.

<< Previous      Next >>      Cancel

After the device reboots with the saved system configuration, the WebUI login prompt appears. For information on how to access the device using the WebUI, refer to “Using the WebUI” on page 29.

# Index

## A

AAL5 multiplexing.....	41
ADSL	
configuring interface .....	41
connecting the cable .....	24
connecting the port .....	24
Annex A .....	24
Annex B .....	24
antennae.....	26
ATM Adaptation Layer 5.....	41

## B

backup interface to Untrust zone .....	37
--	----

## C

cables	
ADSL.....	24
basic network connections.....	23
serial.....	24
certifications	
EMC (Emissions) .....	59
EMC Immunity .....	59
European Telecommunications Standards Institute (ETSI) .....	59
safety.....	59
T1 Interface .....	60
configuration	
admin name and password.....	33
administrative access .....	35
ADSL 2/2 + mini-PIM .....	41
backup untrust interface.....	37
bridge groups (bgroup).....	34
date and time .....	34
default route .....	36
E1 mini-PIM.....	46
host and domain name.....	36
ISDN mini-PIM .....	45
management address.....	36
management services .....	35
T1 mini-PIM.....	46
USB .....	18
V.92 Modem mini-PIM.....	47
virtual circuits.....	42
VPI/VCI pair .....	42
wireless and Ethernet combined .....	40

wireless authentication and encryption .....	38
connection, basic network .....	23

## D

default ip addresses.....	32
---------------------------	----

## I

ISP IP address and netmask.....	44
---------------------------------	----

## L

LEDs	
activity link on Ethernet ports.....	13
PIM 1 .....	11
PIM 2 .....	12
POWER .....	11
STATUS .....	11

## M

management	
through a console .....	28
through a Telnet connection.....	30
through the WebUI .....	29
memory upgrade procedure .....	54
Mini-PIM	
blank faceplate .....	52
installation .....	53
removal .....	52
multiplexing, configuring.....	42

## P

Point-to-Point Protocol over ATM	
<i>See</i> PPPoA	
Point-to-Point Protocol over Ethernet	
<i>See</i> PPPoE	
PPPoA .....	41
PPPoE.....	41

## R

radio transceivers	
WLAN 0 .....	16
WLAN 1 .....	16
reset pinhole, using .....	49

**S**

static IP address..... 41

**U**

Untrust zone, configuring backup interface..... 37

**V**

Virtual Path Identifier/Virtual Channel Identifier

*See* VPI/VCI

VPI/VCI

configuring ..... 42

values ..... 41

**W**

wireless

antennae..... 26

using the default interface ..... 26

WLAN LEDs

802.11a..... 12

b/g..... 12